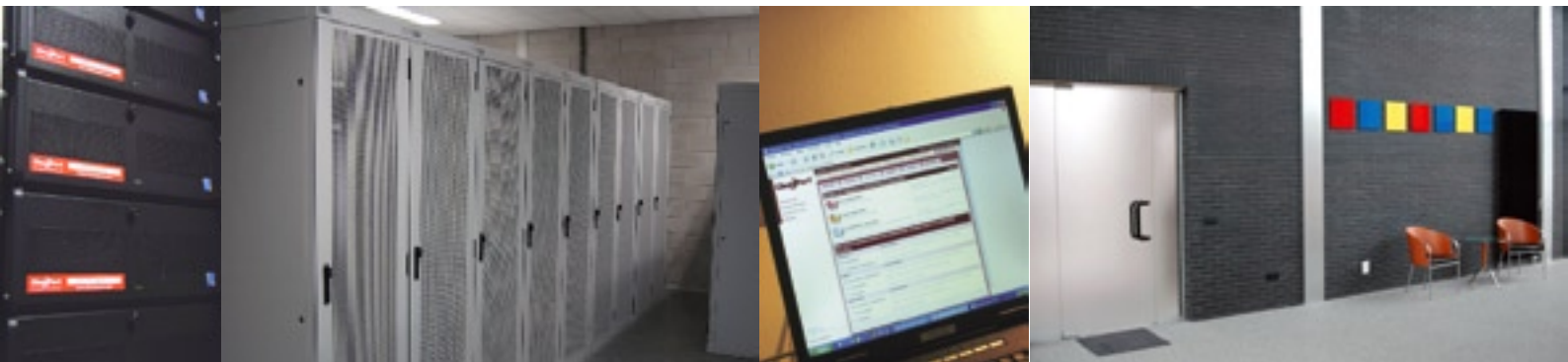


VEELGESTELDE VRAGEN

CLEANPORT MEF

Veel gestelde vragen



ALGEMENE VRAGEN – DEEL I

Zodra een account in het CleanPort systeem is aangemaakt, wat moet er dan nog gebeuren om de mail van de klant te laten filteren?

Om een account te gaan gebruiken moet voor het betreffende domein een eenmalige DNS wijziging plaatsvinden. Deze wijziging betreft het aanpassen van de MX records (zoals aangeven in de "Implementatie handleiding") zodat de inkomende e-mail voor het betreffende domein op een CleanPort mail tower binnenkomt. Hier wordt de mail vervolgens gecontroleerd en gefilterd en worden de virussen en spam e-mails in quarantaine gezet vervolgens worden de overige e-mails op de mail server van de klant afgeleverd.

Wanneer een klant aangeeft geen mail te ontvangen, welke controles uit te voeren?

1. De meest voorkomende oorzaak is de bereikbaarheid van de mail server van de klant
2. Updates/wijzigingen in de firewall bij de klant willen nog wel eens voor problemen zorgen
3. Staan de MX records voor het domein van de klant wel goed, dit is de controleren door in de loggen op de "Management Tool Myaccount" als gebruiker of reseller, deze informatie wordt getoond onder het tabblad "Services"

CleanPort monitort haar systemen 24 uur per dag, waarbij er "thressholds" voor beschikbaarheid en queue hoeveelheden zijn waarbij het support team pro-actief wordt gewaarschuwd. Mochten de bovenstaande controles geen resultaat opleveren, neem dan contact op met het support team, per e-mail support@nl.cleanport.com of per telefoon +31 314 39.99.33.

Mocht u suggesties hebben voor ons product development, waar kunt u dan terecht?

Wanneer u ideeën heeft ter verbetering van ons product dan kunt u deze sturen naar: productdevelopment@nl.cleanport.com. Uw suggesties worden vervolgens beantwoord en u ontvangt van ons een reactie.

Waar kan er worden ingelogd op de "Management Tool MyAccount"?

Inloggen op de "Management Tool MyAccount" kan via de URL: <https://myaccount.cleanport.com>, er kan op gebruikers en reseller niveau worden ingelogd. Voor resellers bestaat de mogelijkheid om gebruik te maken van een "customized" versie van de "Management Tool MyAccount". Er zal dan gebruik gemaakt worden van een andere URL.

Wat gebeurt er met de mail wanneer de mailserver van een klant tijdelijk niet bereikbaar is?

Wanneer het de "CleanPort Mail Tower" niet lukt om mail bij de klant af te leveren zal deze het met verschillende tijdsintervallen opnieuw blijven proberen. Pas na 7 dagen zal het bericht definitief terug worden gestuurd naar de afzender met de melding dat het bericht niet kon worden afgeleverd.



ALGEMENE VRAGEN – DEEL II

Is het noodzakelijk om naast CleanPort nog andere maatregelen te nemen om virussen buiten het bedrijfsnetwerk te houden?

Veruit het merendeel van de virussen komen via e-mail binnen, door CleanPort te gebruiken is uw e-mail effectief beschermd tegen virussen en spam. Wanneer u echter regelmatig gebruik maakt van diskette's of cd-rom's die u van klanten ontvangt of uit uw eigen archief is het raadzaam hiervoor een virusscanner te installeren, zodat deze de data op de externe gegevensdragerseerst kunnen controleren.

Wat is een open-relay en wat zijn de mogelijke gevolgen ervan?

Een open-relay server staat het toe om mail te versturen naar derden, waardoor een kwaadwillende een "open-relay" server kan misbruiken om spam te versturen. Dit is uiteraard een onwenselijke situatie, een mailserver hoort alleen mail te ontvangen voor 1 of meerdere geconfigureerde domeinen. Daarnaast zou een server alleen mail moeten versturen vanaf het eigen domein en/of geconfigureerde adressen.

Hoe kan ik controleren of een mail server een open-relay is?

Er is een online test beschikbaar om te controleren of een bepaalde server een open-relay is, zie hiervoor <http://www.abuse.net/relay.html>.

Zorgt het scannen van mail door CleanPort voor een vertraging in de aflevering?

Het scannen van berichten kosten gemiddeld minder dan 1 seconden. De gemiddelde tijd tussen het ontvangen van een bericht door CleanPort en de eerste poging deze af te leveren op de mail server van de klant is gemiddeld minder dan 1 seconden. De vertraging is afhankelijk van de grootte van het bericht en eventuele pieken in het mail verkeer. Het komt zelden voor dat de verwerkingstijd meer dan een aantal seconden bedraagt.

Is het mogelijk de maximale grootte van e-mails in te stellen?

Standaard is de maximale grootte van een e-mail 25Mb, e-mail die groter zijn worden niet geaccepteerd. Mocht u deze grootte willen aanpassen dan kan dit door gebruik te maken van de "Geavanceerde instellingen" van de ContentFilter. Hier kan bijvoorbeeld worden ingesteld dat het hele domein of een bepaalde gebruiker maar e-mails tot 5Mb mag ontvangen.



VRAGEN MET BETREKKING TOT FILTERING – DEEL I

Wat gebeurt er met onderschepte virussen, spam en berichten die door de Content Filter worden detecteert?

Standaard worden onderschepte virussen en spam berichten in quarantaine geplaatst. De klant kan in de "Management Tool MyAccount" ook aangeven dat deze berichten direct worden verwijderd. Voor onderschepte spam en berichten die door de content filter worden gedetecteerd kan men er ook voor kiezen het onderwerp te laten uitbreiden met *** SPAM *** of *** CF ***. Op deze manier kan er op de mail server van de klant of in de mail software op de desktop zelf worden bepaald hoe deze gemarkeerde berichten worden afgehandeld. Doordat de berichten gemarkeerd zijn biedt het de mogelijkheid om ze in aparte folders te archiveren.

Hoe lang blijven virussen en spam in de quarantaine opgeslagen?

Virussen worden standaard 14 dagen bewaard in de Virus Quarantaine, voor spam en berichten die door de Content Filter worden gedetecteerd geldt een bewaartermijn van 30 dagen. De drie afzonderlijke quarantaines zijn op gebruikersniveau te benaderen via de "Management Tool MyAccount". In de quarantaines kunnen berichten ook handmatig worden verwijderd, tevens bieden de quarantaines verschillende sorteerfuncties en een zoekfunctie om gemakkelijk berichten terug te vinden.

Wat kan ik doen wanneer er berichten onterecht worden tegengehouden en in de quarantaine staan?

De SpamFilter gevoeligheid kan op 5 niveau's worden ingesteld, wanneer de SpamFilter op het hoogste gevoeligheidsniveau wordt ingesteld zal het een groot gedeelte van de technisch slecht opgestelde nieuwsbrieven tegengehouden. Wanneer u deze e-mails toch zou willen ontvangen kunt u ze vrijgeven uit de quarantaine. U kunt ook aangeven of dit bericht moet worden onthouden als "niet spam", dit zorgt ervoor dat er een "signature" van dat bericht en het afzenderadres worden onthouden, zodat bij een soortgelijk bericht deze wordt doorgelaten.

Wat te doen wanneer u regelmatig spam of een virus ontvangt?

Wanneer de mail server van de klant niet gefirewalled of dusdanig is ingesteld dat er alleen mail wordt geaccepteerd vanaf de CleanPort Mail Tower is de kans aanwezig dat er mail langs de filters heen direct op de mail server van de klant wordt afgeleverd. In de "Implementatie handleiding" staat omschreven hoe dit ingesteld kan worden.

Wanneer de mail server en/of firewall juist zijn geconfigureerd en u ontvangt toch regelmatig spam?

Alhoewel het zelden voorkomt kan het zijn dat u een bepaald soort spam ontvangt (die weinig voorkomt) en niet door onze SpamFilter wordt tegengehouden, dit is echter ook afhankelijk van de gevoeligheid die gekozen is voor de SpamFilter. U kunt van deze berichten de "mail source" sturen naar support@nl.cleanport.com, u ontvangt vervolgens van ons een reactie.

VRAGEN MET BETREKKING TOT FILTERING – DEEL II

Hoe uitgaande e-mail filtering voor een klant in te stellen?

Niet alle klanten willen hun uitgaande e-mail ook laten filteren, voor de klanten die dit wel willen wordt deze mogelijkheid geboden. Door een of meerdere IP nummers aan een domein te koppelen via de "Management Tool MyAccount" onder "Relay" kan de klant vanaf deze IP nummers via de CleanPort Mail Tower mail versturen. Dit wordt in de "Implementatie handleiding" uitgebreider omschreven.

Wat is "mail source" en wat zijn "mail headers" en hoe deze te lezen?

Onder "mail source" wordt de gehele broncode van de mail verstaan. In een mail programma zoals Outlook wordt maar een gedeelte hiervan getoond, het gedeelte wat getoond wordt heet de "mail body", het gedeelte wat niet (direct) getoond wordt heet de "mail headers". Uit de mail headers valt onder meer op te maken wat het onderwerp van een mailtje is. Daarnaast bevat de "mail header" informatie over de route die een e-mail heeft afgelegd om op de eindbestemming uit te komen, en informatie over de afzender en geadresseerde. Wanneer een mailtje onterecht niet tegengehouden zou zijn kunnen wij met de "mail source" analyseren waarom dit niet gebeurd zou zijn.

Wat gebruikt CleanPort om effectief virussen tegen te houden?

CleanPort maakt gebruik van verschillende anti-virus engines, waaronder onze eigen engine genaamd "ProTAG". Deze heuristische engine herkent pro-actief nieuwe virussen op basis van patronen en herkenningsregels. Met de combinatie van scanners wordt een optimaal resultaat behaald.

Het ontvangen van notificaties bij het blokkeren van virussen?

Er kan per gebruiker of domein worden aangegeven of er notificaties moeten worden verstuurd wanneer een virus wordt tegengehouden. Deze notificatie wordt gestuurd naar het adres waar het virus aan gericht was en (wanneer ingesteld) het e-mail adres van de domeinbeheerder.

Waarom wordt er niet de mogelijkheid geboden om ook de afzenderadressen een notificatie te sturen?

Bijna alle virussen van de laatste jaren maken gebruik van "spoofed" afzenderadressen. Het afzenderadres is dus niet het echte adres van de afzender, het is of een adres verzameld op de computer van het slachtoffer of een willekeurig gekozen afzenderadres. Het versturen van een notificatie naar een "spoofed" adres zou nutteloos, en kunnen worden aangemerkt als spam.

Welke mogelijkheden zijn er om berichten tegen te houden naast de automatische detectie van e-mails?

Zowel de SpamFilter en ContentFilter bieden de mogelijkheid om "rules" aan te maken, met behulp van de "Geavanceerde instellingen". De mogelijkheden bestaan o.a. uit het blokkeren van afzenderadressen, afzenderdomeinen en IP adressen. Daarnaast is het mogelijk bestandstypes te blokkeren en op gedeeltes van het ontwerp of berichten te blokkeren.

CleanPort Nederland B.V.

Gildenbroederslaan 1, Doetinchem

Postbus 110
7000 AC DOETINCHEM
The Netherlands

Tel: +31 314 39 99 33
Fax: +31 314 39 99 34
email: info@nl.cleanport.com

www.cleanport.com

