Dienstbeschrijving
E-mailservice

RoutIT

Datum: 28-11-2016

Versielog RoutIT

Start document RoutIT	Onbekend
1e versie in gebruik bij CBG Connect	Juli 2015
Algehele update RoutIT	28-11-2016

Inhoudsopgave

1 Inleiding

E-mail is niet meer weg te denken als communicatiemiddel in onze maatschappij. Zowel zakelijk als privé is er grote behoefte aan een 24-uurs beschikbaarheid van emaildiensten. Echter ondervinden bedrijven en consumenten steeds meer last van ongewenste e-mail. Dat is niet zo vreemd omdat ruim negentig procent van alle verzonden e-mails ongewenst is. RoutIT biedt de meest innovatieve oplossing op het gebied van e-maildiensten.

RoutIT biedt de meest innovatieve oplossing op het gebied van e-maildiensten. De nieuw ontwikkelde anti-spam oplossing van RoutIT levert spectaculaire resultaten op. De anti-spam filter is het summum op het gebied van beveiliging. RoutIT maakt voor deze anti-spam dienst gebruik van de appliances van Ironport.

Deze dienstbeschrijving beschrijft de RoutIT mail service.

2 Inhoud van de dienst

De RoutIT e-mail dienst geeft de klant van CBG Connect de mogelijkheid om e-mailberichten te ontvangen door middel van SMTP of POP3 e-mail accounts. RoutIT heeft bij deze dienst een portal ontwikkeld waarin het mogelijk is voor CBG Connect om voor uw e-mail account een aantal zaken te bepalen, zoals eigenschappen van de mailboxen bij POP3 en SMTP. Bij het afnemen van een RoutIT spam filter dienst is het zelfs mogelijk de gevoeligheid van de spam controle in te stellen.

Bestaande accounts migreren
Misschien bent u al in het bezit van een RoutIT e-mail account. Deze accounts zijn niet allemaal te migreren. Het is mogelijk om een huidig SMTP account te migreren. Voor POP3 e-mailboxen zal een nieuwe aanvraag moeten worden ingediend.

Nieuw mail service aanvragen
Om deze nieuwe dienst te bestellen voor koppelen van domeinen kunt u contact opnemen met CBG Connect.

User interface
Voor het beheren van de accounts is een speciale portal ontwikkeld. Deze portal is zowel door de partner als door de klant te gebruiken. In deze portal kunt u diensten aanvragen en SMTP en POP3 diensten aanpassen. Daarnaast is er ook een log beschikbaar om te zien welke wijzigingen er zijn gemaakt binnen de portal.

Wat kan ik als CBG Connect instellen?
Met de gebruikersnaam en wachtwoord vanuit IRMA kan CBG Connect inloggen op de mail portal. Hier kan CBG Connect voor klanten eigenschappen van de SMTP en POP3 mailboxen aanpassen, mailboxen aanmaken of verwijderen.

Wat kan ik als klant instellen?
De mailportal https://james.routit.net/MailService/ is los van de RoutIT portal ontwikkeld. Deze is ook vanaf een directe url beschikbaar. Omdat de mail portal los staat van de RoutIT portal is het mogelijk om zelf met een gebruikersnaam en wachtwoord de eigenschappen van de SMTP en POP3 mailboxen te veranderen.

Opzeggen maildiensten
Wanneer u een domeinregistratie order opzegt, wordt de facturatie van deze order beëindigd, met inbegrip van een maand opzegtermijn. De mailafhandeling van dat domein blijft echter gewoon actief totdat de koppeling tussen de mailservice en het domein verbroken wordt. De domainhandling blijft gefactureerd worden totdat deze koppeling verbroken wordt.
Om de domainhandling te onderbreken tijdens de opzegtermijn dient het domein ontkoppeld te worden van de mail dienst. Om de domainhandling voor Mail SMTP diensten te kunnen onderbreken moet RoutIT de dienst technisch onklaar maken. Neem contact op met CBG Connect zodat zij een ticket aan kunnen maken op de betreffende maildienst.

3 Werking

Kenmerken van de e-mailservice

- Geografisch-Redundant uitgevoerd mailplatform.
- SenderBase Reputatie filtering (http://senderbase.org)
- CASE Anti-Spam engine (content filtering)
- Sophos Anti-virus scanning.
- Het mail platform gebruik de IP range 89.146.30.0/27 voor het versturen van mail.

MX Record Configuratie

Voor het gebruik van e-maildiensten (inkomend) dienen de MX records bij gebruik van POP3 & SMTP services binnen de zone op de volgende manier te worden geconfigureerd.

Prefix	Servers
10	Smtp.routit.net
20	Smtp1.routit.net

Uitgaande mail (smarthost/relay) configuratie

Als u gebruik wilt maken van de door RoutIT beheer uitgaande mailservers kunt u gebruik maken van smtp.routit.net in uw client of op uw server. Houd er rekening mee dat het Senderbase Reputatie filter ook van toepassing is op RoutIT verbindingen. Zie voor meer informatie ook het onderdeel "Senderbase Reputatie Filtering". De uitgaande servers van RoutIT kunnen alleen gebruikt worden vanaf een RoutIT verbinding en ondersteunen geen authenticatie.

Content-Filtering (CASE)

Alle e-mail diensten zijn aan te vullen met een content-filtering. De aangeboden e-mail zal worden gecontroleerd op content. Naar aanleiding van de inhoud van het bericht zal er een spam score aan het bericht worden toegekend. De partner of eindgebruiker heeft de mogelijkheid om per account aan te geven welke actie dient te worden genomen.

Content-filtering kent een score van 0-100 toe aan een bericht waarbij het 100 gegarandeerd SPAM is en 0 gegarandeerd legitiem. Onderstaand de niveaus/levels welke wij hanteren in verhouding tot de scores:

Level 0
  Suspected Spam vanaf score: 50
  Spam vanaf score: 95
Level 1
  Suspected Spam vanaf score: 50
  Spam vanaf score: 90
Level 2
  Suspected Spam vanaf score: 50
  Spam vanaf score: 85
Level 3
  Suspected Spam vanaf score: 50
  Spam vanaf score: 80
Level 4
  Suspected Spam vanaf score: 50
  Spam vanaf score: 75
Level 5
  Suspected Spam vanaf score: 50
  Spam vanaf score: 70

In geval er aan 1 van de drempelwaardes wordt voldaan kunnen de volgende "onderwerp" wijzigingen worden doorgevoerd:

Suspected actie: "[SUSPECTED]" wordt aan het onderwerp toegevoegd en het bericht wordt gewoon afgeleverd.
Spam actie: "[SPAM]" wordt aan het onderwerp toegevoegd en het bericht wordt doorgezet naar de quarantaine.

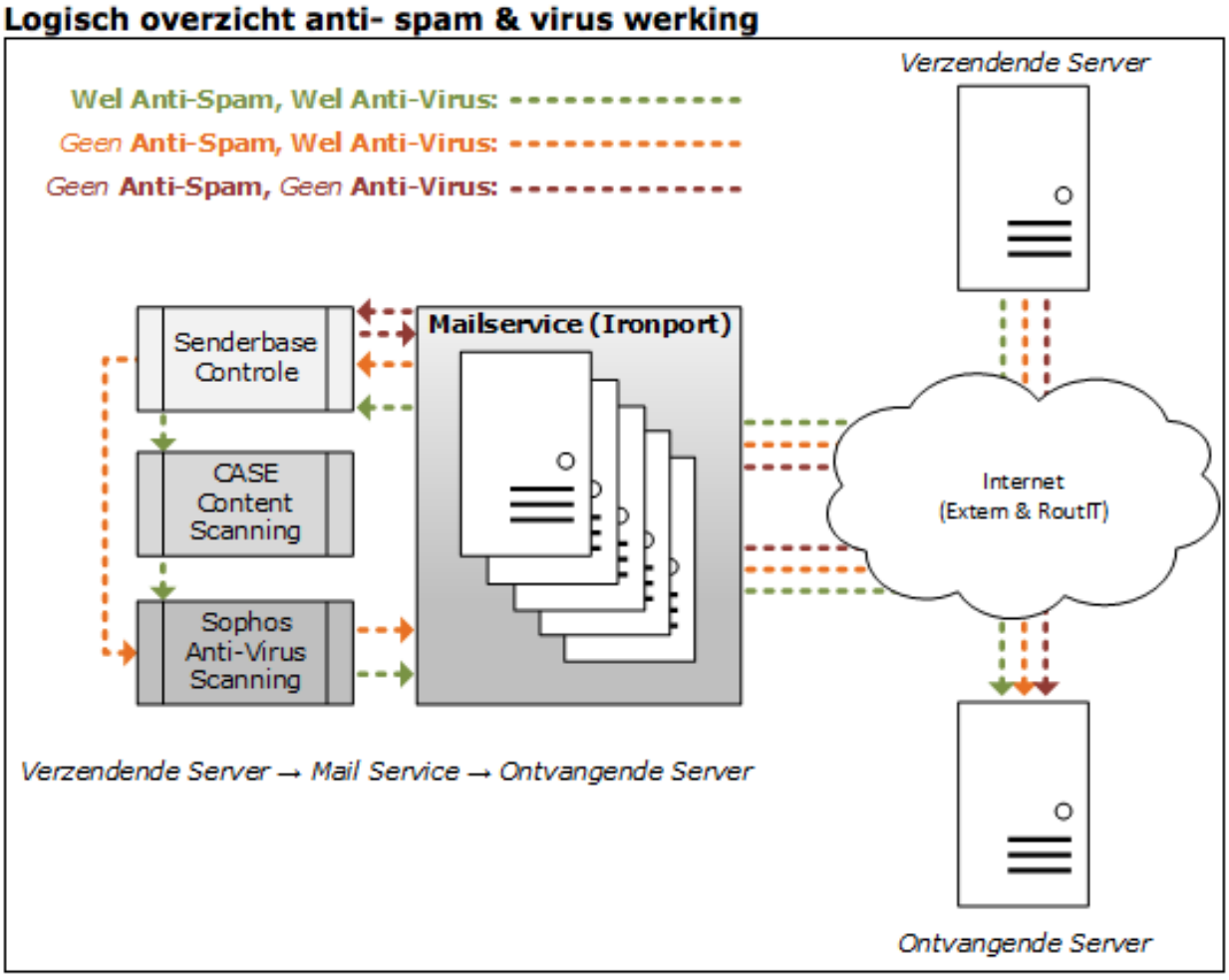
Anti-Virus (Sophos)
Virussen zijn een steeds grotere bedreiging. RoutIT biedt de mogelijkheid om besmette bestanden bij binnenkomst op de mailservers direct op te schonen of te verwijderen. Virrusscans zijn uiteraard geen garantie maar door de laatste technieken te gebruiken hopen wij het risico tot een minimum te beperken.

Wanneer er een virus-wordt aangetroffen in een bericht zullen de Ironport's deze initieel pogen uit een bericht te verwijderen en vervolgens het schone bericht afleveren. Is dit niet mogelijk dat zal het bericht naar de quarantaine gaan. Daarnaast zijn er ook bestanden niet gescanned kunnen worden:

** Bestanden welke met een wachtwoord/encryptie zijn uitgerust.
** Bestanden groter dan 30Mb.

Senderbase Reputatie Filtering
De Senderbase reputatie is een soort dynamische blacklist welke op basis van wereldwijd vergaarde gegevens bepaald hoe betrouwbaar een IP adres is. Deze gegevens worden samengevat in een score van +10 tot -10 waarbij +10 extreem betrouwbaar is. RoutIT voert op basis hiervan blokkades uit op inkomende connecties naar het platform ongeacht of er gebruikt word gemaakt van de aanvullende services (anti- spam en/of virus).

Doordat Senderbase gebruik maakt van de wereldwijd vergaarde informatie van duizenden Ironport's is het een van de meest betrouwbare blacklisting mechanismes van vandaag. Daarnaast is het beheersmatig ook minder intensief dan de "oude" methodes middels DNS blacklists omdat er geen delisting procedures zijn. Een host kan vanzelf weer mail versturen aan de wereld als deze wordt opgeschoond en enkel nog "schone" mail stuurt (hiermee zal zijn score weer omhooggaan).



Blacklists
Blacklist zijn lijsten waarop IP adressen, netwerken, domeinen of e-mail adressen bijgehouden worden. Deze worden opgenomen op de blacklist omdat er spam, virussen vanaf verstuurd worden, ze open staan voor relay, enz.

De reden waarom een adres op een lijst wordt opgenomen verschilt per lijst. Deze is te achterhalen door de listing policy van de blacklist te raadplegen op de website van de beheerder.

Op de website is vaak een query tool beschikbaar, waarmee gekeken kan worden of een adres is opgenomen op de lijst, een Removal Request Form en de delisting policy.

RoutIT maakt gebruik van verschillende lijsten. Op de lijsten die door RoutIT gebruikt worden staan uitsluitend IP-adressen. Zodra het IP adres van de afzender voorkomt op één van deze lijsten, wordt de mail niet geaccepteerd. Voor lijsten met een trage removal procedure is ook een ‘negatieve´ Senderbase Reputation Score vereist, voordat de mail geweigerd wordt.

De door RoutIT gebruikte Blacklists zijn:

sbl-xbl.spamhaus.org.
CBL

4 Ironport Outlook Plug-in

Cisco/Ironport Email Security is een plug-in die gebruikt kan worden in combinatie met Microsoft Outlook. Eenmaal geïnstalleerd zal er een extra "ribbon" onderdeel beschikbaar zijn om deze plug-in te gebruiken. Dit onderdeel stelt u in staat rechtstreekse rapportages te versturen naar Cisco/Ironport over geselecteerden berichten in uw mailbox.

De rapportages die u verstuurt, worden gebruikt om de filters van de door Ironport aangedreven relay hosts van RoutIT te updaten met de laatste bericht kenmerken. De berichtrapportages worden samengesteld op basis van de volgende opties:

Spam
Hiermee zorgt u ervoor dat dit bericht in de toekomst wordt gekenmerkt als spam, in het uitzonderlijke geval deze uw mailbox toch heeft bereikt.
Not spam
Mocht u constateren dat een bericht onterecht als "[SUSPECT SPAM]" wordt beschouwd, kunt u hiermee kenbaar maken dat dit een legitiem bericht is.
Virus
Ondanks dat RouTIT voor anti-virus gebruikmaakt van de laatste Sophos virusdatabase en scantechnieken, kan er in een uitzonderlijk geval toch een virusbericht worden ontvangen wanneer deze nog niet bekend is in de database. Door deze te rapporteren zal het bericht worden onderzocht en in de toekomst worden opgeschoond, alvorens deze wordt ontvangen.
Phishing
Dit zijn vaak valse berichten van banken (of andere instellingen) en worden veelal gekenmerkt doordat zij uw persoonlijk gegevens middels malafide sites proberen te ontfutselen. Mocht u of uw klant dergelijke berichten tegenkomen, kunnen deze berichten worden gerapporteerd. Hierdoor worden de filters op basis van deze kenmerken geüpdatet en zullen deze in de toekomst worden geblokkeerd.

Houd u er rekening mee dat u ook gebruik dient te maken van een "Mail Service", welke zowel Anti-Spam als Anti-Virus heeft ingeschakeld. Enkel op die manier worden uw berichten gecontroleerd met de technieken die gebruikmaken van deze filters.

5 Service Level Agreement

Deze dienst is beschikbaar in de volgende Service Level Agreements:

Dienst	SLA B	SLA N	SLA A
E-mailservice	X		

Meldingen werkzaamheden en storingen
Werkzaamheden met impact op de beschikbaarheid van de dienst worden altijd gemeld op de website http://www.cspreporter.nl/. Deze website is publiekelijk beschikbaar.

Indien mogelijk streeft RoutIT ernaar de melding tenminste 7 dagen voor de werkzaamheden te publiceren.

Service Level Agreements
Een Service Level Agreement (SLA) is een overeenkomst tussen opdrachtgever en opdrachtnemer waarin de afspraken over het niveau van de dienstverlening zijn vastgelegd.

6 Algemene kaderzetting van deze dienstbeschrijving

Deze dienstbeschrijving vormt een onlosmakelijk deel van de ondertekende offerte in combinatie met Algemene Voorwaarden CBG Connect, de Algemene Voorwaarden Service Provider RoutIT en mogelijke bedrijfsspecifieke voorwaarden en afspraken en productbrochures.

De informatie in deze dienstbeschrijving is gelijk aan de informatie van Service provider RoutIT

CBG Connect behoudt zich het recht voor deze dienstbeschrijving zonder voorafgaande melding te wijzigen.

De dienstbeschrijving is uitsluitend bestemd voor intern gebruik binnen uw organisatie. Het maakt onderdeel uit van het contract tussen u en CBG Connect. Het document is aan u verstrekt om een afgewogen keuze te kunnen maken voor CBG Connect als leverancier van deze dienst.

CBG Connect B.V., januari 2017