16. MailPlus Server

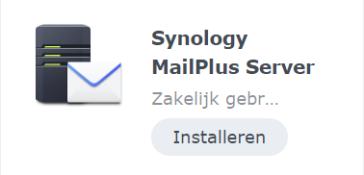
Een mooie applicatie om te gebruiken is MailPlus Server. Deze applicatie van Synology stelt u in staat om uw eigen e-mailserver te installeren en te beheren. Het fijne hiervan is, dat u compleet onafhankelijk bent van iedereen en dat uw e-mail alleen door u kan worden bekeken. De applicatie bestaat uit twee onderdelen. Met de Synology MailPlus Server stelt u alles in en Synology MailPlus is uw e-mailprogramma. Wat u wel van tevoren moet weten, is dat uw bij de standaard installatie maar vijf e-mailadressen kunt gebruiken. Wilt u meer e-mailadressen in gebruik nemen, dan zult u extra licenties moeten aanschaffen.

Om een eigen e-mailserver te draaien hebt u een eigen domeinnaam nodig. Die kunt u al hebben voor vier euro per jaar. Let er bij het kiezen van een provider op, dat het u vrij staat om de DNS-records van het gekozen domein zelf aan te passen. Het inregelen van de e-mailserver is de eerste keer best wel lastig. Om die reden heb ik in dit hoofdstuk daar extra aandacht aan besteed, want het moet wel veilig gebeuren.

Een eigen e-mailserver brengt ook gevaren met zich mee, want hackers willen hier maar al te graag gebruik van maken, om op die manier duizenden spam-berichten te kunnen versturen. Om dit te voorkomen zult u zich moeten verdiepen in alle beveiligingsopties die de MailPlus Server biedt. Draait alles naar wens, dan kunt u met elk e-mail-programma de e-mail ontvangen, online webmail gebruiken van Synology of op uw telefoon gebruik maken van de MailPlus app.

16.1 Installatie Synology MailPlus Server

1. Ga naar het Package Center, zoek op mail en installeer Synology MailPlus Server.



2. Open MailPlus Server na de installatie.

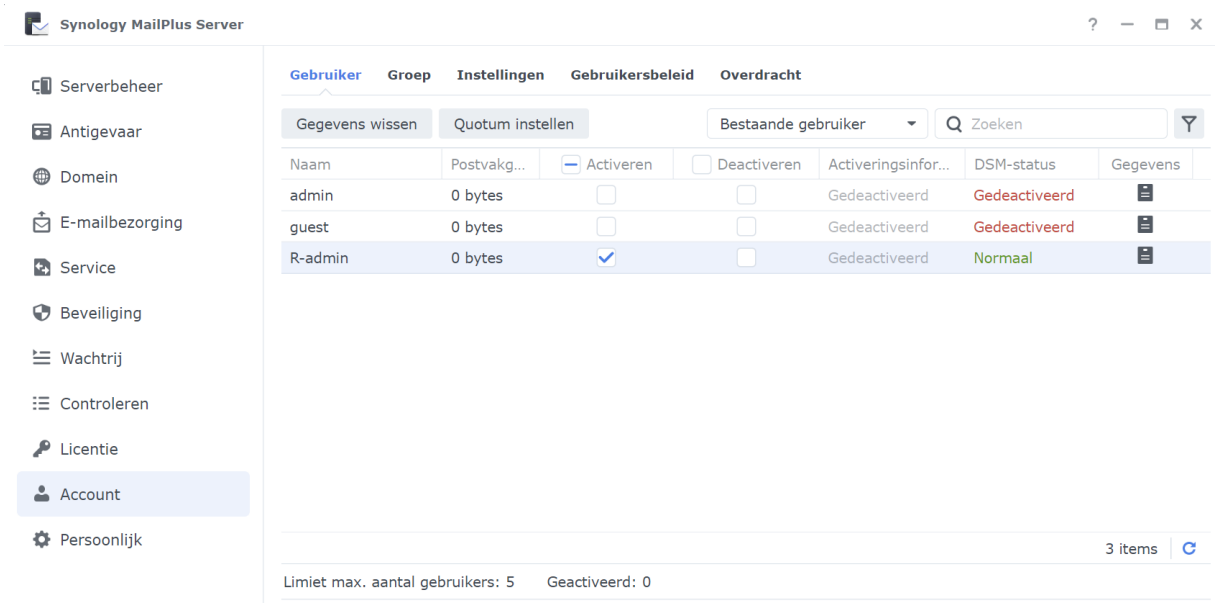
3. Kies voor de standaard optie Een nieuw e-mailsysteem maken. Klik op Volgende.

4. Vul bij Domeinnaam het domein in waarop u de e-mail wilt ontvangen. Vul bij Hostnaam (FQDN) het PTR-record in dat u krijgt via uw internetprovider. Een PTR-record (Pointer Record) is hetzelfde als rDNS oftewel Reverse DNS. Het geeft aan dat de hostnaam die u gebruikt daadwerkelijk is gekoppeld aan het IP-adres dat u van uw Internetprovider hebt gekregen. Veel mailservers voeren een check uit om dit te controleren. Is reverse DNS niet ingesteld, dan kan uw e-mail geweigerd worden of in de spambox terecht komen. Hebt u niet de mogelijkheid om een PTR-record te verkrijgen, dan zijn er nog een aantal andere manieren om door deze

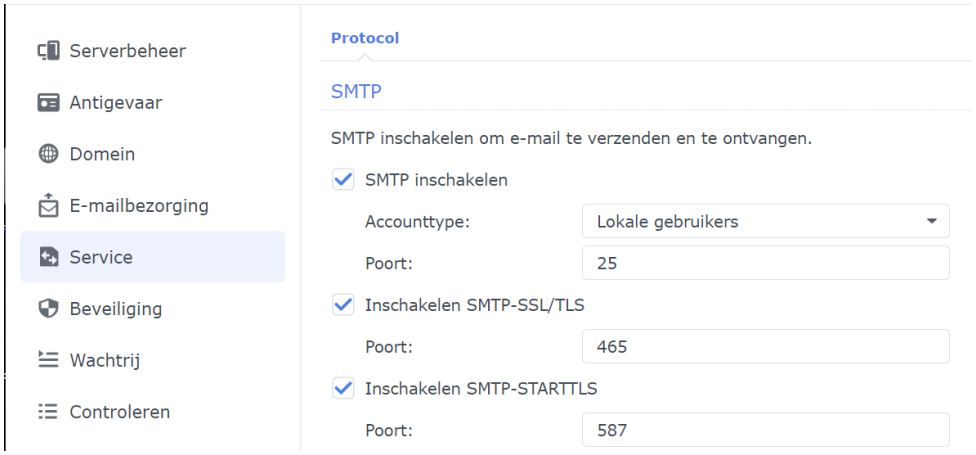
check heen te komen. Hier kom ik later op terug. Omdat het veld wel moet worden ingevuld, geeft u hier uw domeinnaam op. Klik op Volgende.

5. U krijgt een samenvatting. Klik op Toepassen. De instellingen worden uitgevoerd.

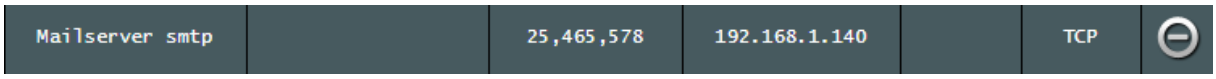
6. Klik op Voltooien.
7. Klik aan de linkerkant op Account en activeer de accounts die gebruik mogen maken van de e-mailserver. Zonder extra licenties mag u vijf accounts activeren. Klik op Toepassen.



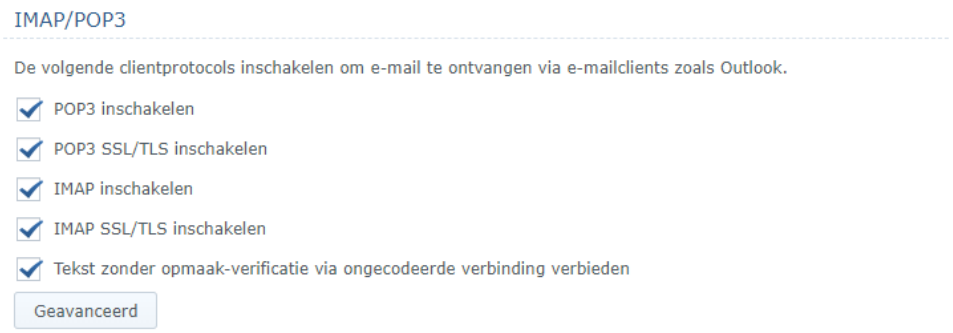
8. Klik aan de linkerkant op Service.



9. Onder het kopje SMTP (Simple Mail Transfer Protocol) staan er al vinkjes bij SMTP, SMTP-SSL en SMTP-TLS. De eerste optie met standaard poort 25 is om e-mail te versturen of te ontvangen via de onbeveiligde poort. Om e-mail te versturen via de beveiligde poorten 465 voor SSL (Secure Socket Layer) en 587 voor het nieuwere TLS (Transport Layer Security) moet er op uw server een SSL-certificaat draaien. Zet deze drie poorten open op uw router.

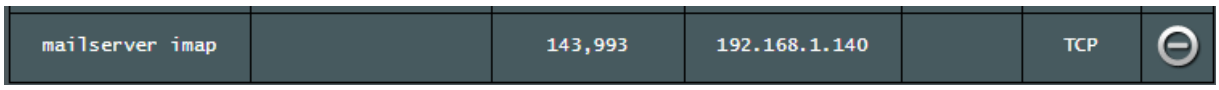


10. Onder het kopje IMAP/POP3 geeft u aan welke cliënt-protocollen er mogen worden gebruikt om e-mail te ontvangen.

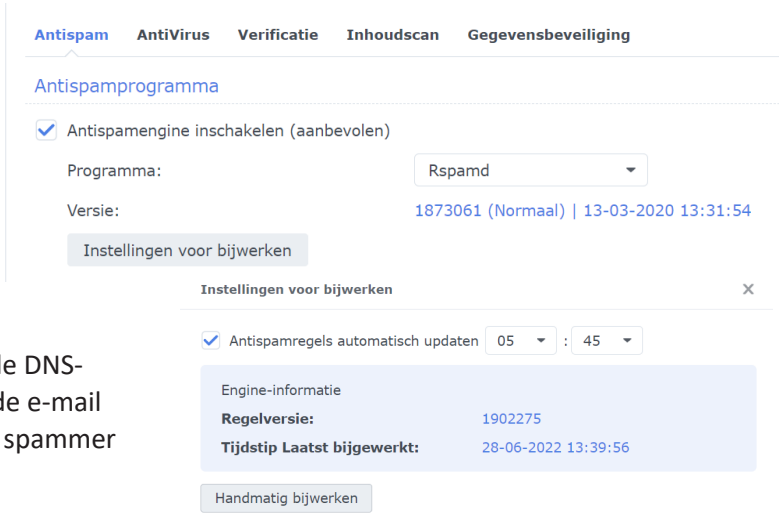


11. Haal de vinkjes weg van de protocollen die u niet wilt gebruiken. Bij het POP3 protocol, haalt u de e-mail van de server. Met de IMAP protocollen blijft de e-mail op de server staan. Wilt u POP3 gebruiken, forward dan de poorten 110 en 995 naar uw NAS.

12. Wilt u IMAP gebruiken, dan routeert u de poorten 143 (onbeveiligd) of 993 (beveiligd) naar uw NAS.

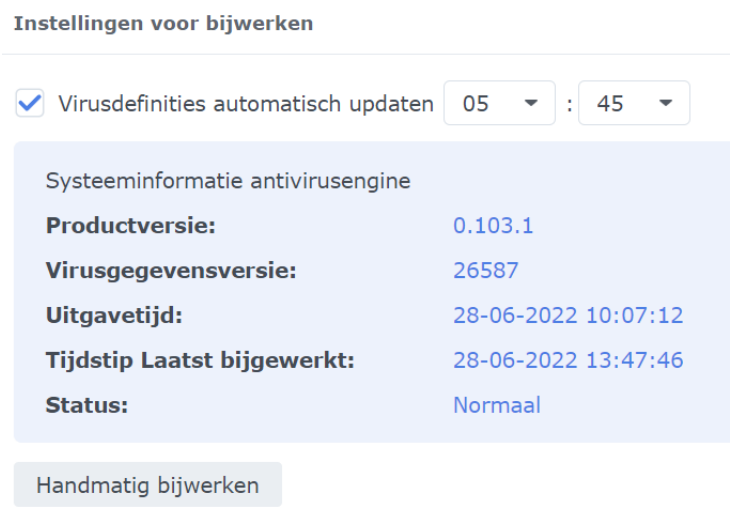


13. Klik aan de linkerkant op Beveiliging. Op het eerste tabblad Spam, schakelt u de Antispamengine in. Klik op Toepassen.
14. Klik op Instellingen voor bijwerken.
15. De Spamregels worden automatisch geüpdatet, maar de eerste keer klikt u op Handmatig bijwerken en daarna op Opslaan.
16. Plaats een vinkje bij DNSBL-instellingen om de DNS-Blackhole List te activeren. De afzender van de e-mail wordt gecontroleerd of die op deze bekende spammer lijst staat. Klik op Toepassen.



17. Ga naar het tabblad AntiVirus en schakel de Antivirusengine in en klik op Toepassen.

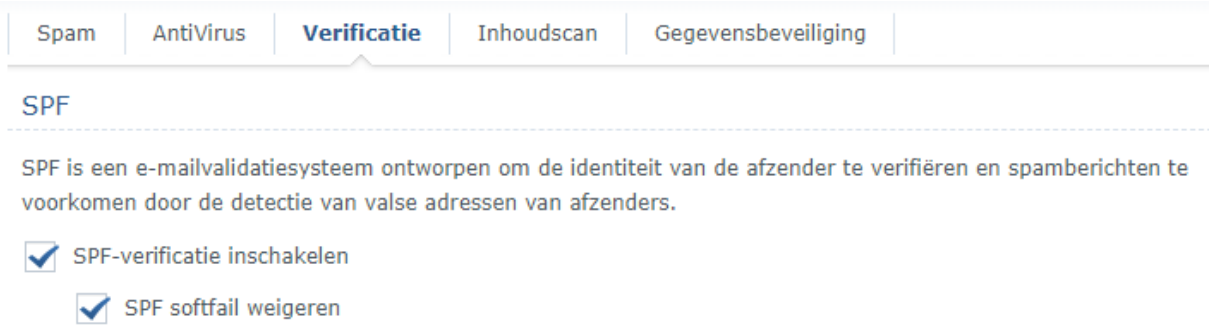
18. Schakel de Google SafeBrowsing-database in om kwaadaardige URL's uit de e-mail te vissen.
19. Activeer de optie om de detectie van malware en phising te verbeteren en Klik op Toepassen.
20. Klik op Instellingen voor bijwerken en klik op Handmatig Bijwerken.



21. Klik op Opslaan. Plaats een vinkje onder Actie bij Onderwerp voorvoegsel toevoegen aan geïnfecteerde e-mailberichten.

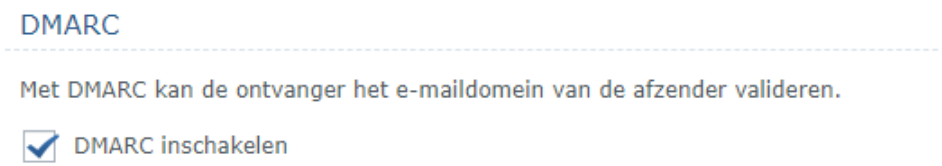
22. Bepaal wat er moet worden gedaan met de e-mails die een virus bevatten. Verwijder deze e-mails, plaats ze in quarantaine, of verstuur ze toch naar het e-mailprogramma. Klik op Toepassen.

23. Ga naar het tabblad Verificatie. Plaats een vinkje bij SPF-verificatie inschakelen (Sender Policy Framework). De mailserver voert nu een check uit om te controleren of de afzender wel mail mag versturen volgens de afzender. De e-mailserver doet een check op de DNS-instellingen. Daar moet een SPF-record staan. Later gaan we dat record ook maken voor uw DNS-instellingen.

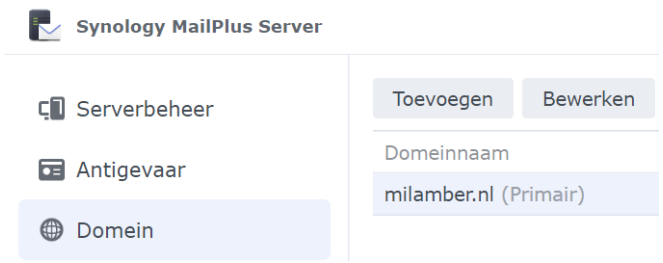


24. Plaats tevens een vinkje bij SPF softfail weigeren om e-mail te weigeren die niet door deze check heenkomen.
25. Plaats een vinkje bij DKIM-verificatie inschakelen voor inkomende e-mailberichten. DomainKeys Identified Mail (DKIM) wordt gebruikt om e-mail te voorzien van een digitale handtekening die is opgenomen in de DNS-instellingen van het domein. Hierdoor kan spam worden tegengegaan.

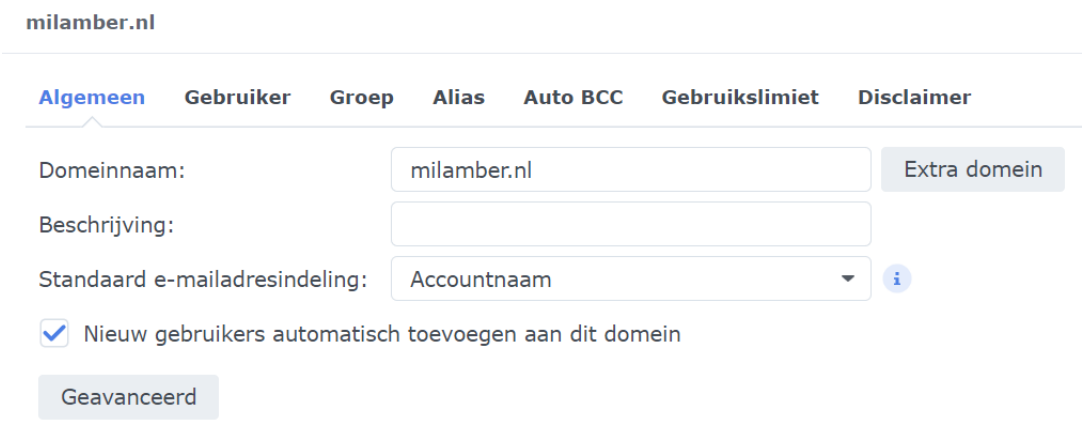
26. De eerste stap voor DKIM is gedaan. Klik op Toepassen.
27. Plaats een vinkje voor DMARC inschakelen.



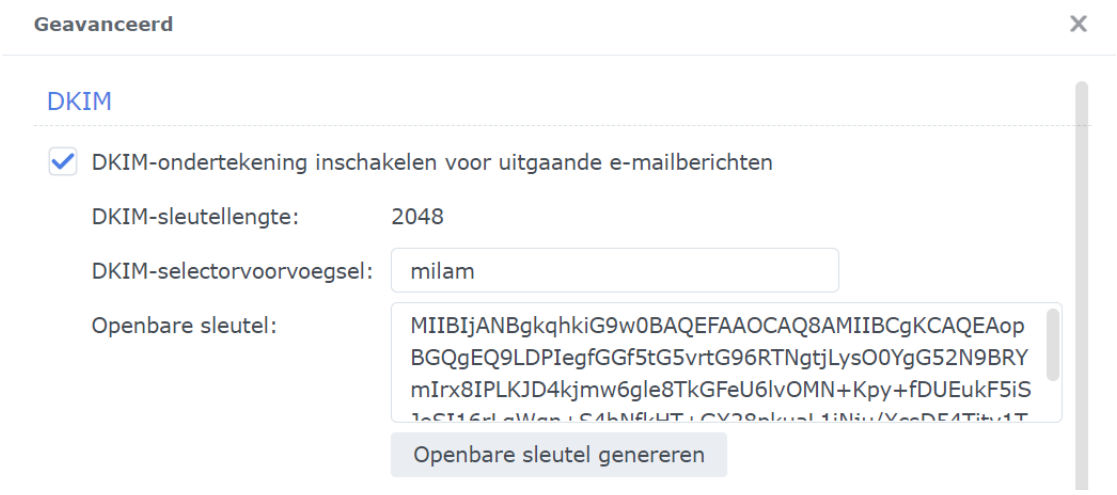
28. Door de Domain-based Message Authentication Reporting and Conformance (DMARC) te activeren kan de ontvangende e-mailserver bepalen wat hij moet doen als uw e-mail niet door de SPF of DKIM check heen komt. Wat de keuze is, wordt bepaald door de DMARC DNS record in je DNS. Klik op Toepassen.
29. Klik aan de linkerkant op Domein.



30. Dubbelklik op het actieve domein.



31. Klik op Geavanceerd en plaats een vinkje bij DKIM-ondertekening inschakelen voor uitgaande e-mailberichten.



32. Geef een naam op bij DKIM-selector voorvoegsel. U hebt die naam zo meteen nodig voor het aanmaken van het DNS-record.
33. Klik op Openbare sleutel genereren. Kopieer de sleutel naar een tekstbestand. U hebt deze sleutel zo meteen nodig voor het DNS-record. Klik op OK en Opslaan.
34. U hebt nu de belangrijkste instellingen ingesteld. Hoogste tijd om nu de DNS-instellingen van uw domein in te stellen.