

Veilig e-mailen

E-mail heeft zich inmiddels ruimschoots bewezen als communicatiemiddel. Het is een snelle en goedkope manier om met anderen waar ook ter wereld te communiceren. Als gevolg hiervan vindt inmiddels een groot deel van onze dagelijkse communicatie, zowel privé als zakelijk, plaats via e-mail. Tussen al die e-mails die dagelijks worden verstuurd bevinden zich ongetwijfeld ook berichten met een vertrouwelijk karakter, waarvan u liever niet heeft dat iemand anders dan de ontvanger ze kan lezen. En u wilt al helemaal niet dat uw berichten worden gewijzigd door een buitenstaander op weg naar de ontvanger.

Waarschijnlijk bent u zich er niet van bewust dat uw e-mail normaal onbeveiligd wordt verstuurd. Dat betekent dat iedereen, die toegang heeft tot de knooppunten die op de weg liggen die uw berichten afleggen naar de e-mailserver, de inhoud van uw bericht kan lezen. In theorie kunnen er op de knooppunten zelfs wijzigingen in berichten worden aangebracht. Bovendien worden uw wachtwoorden als leesbare tekst verstuurd. Dit hoeft voor u niet direct een probleem te zijn, omdat de weg die uw berichten afleggen vaak via vertrouwde partijen loopt (zoals uw internetprovider).

Er zijn echter situaties denkbaar waarin u de verbinding met de e-mailserver van InterNLnet niet wilt of kunt vertrouwen. Dit zal voornamelijk het geval zijn als u via een 'vreemd' netwerk verbindt met het internet. In dat geval kan e-mailen via een beveiligde verbinding de uitkomst bieden. Een tweede probleem waar u tegenaan kunt lopen wanneer u via het netwerk van een andere provider gaat mailen, is dat u geen toegang krijgt tot onze e-mail server. Ook dit probleem is op te lossen door uw e-mail te versturen via een beveiligde verbinding.

Waarom e-mailen via een beveiligde verbinding?

U vertrouwt de verbinding met de e-mailserver van InterNLnet niet

Wanneer u niet via een vertrouwd netwerk met het internet verbonden bent (bijvoorbeeld als u buiten uw eigen kantoor aan het werk bent) of als u verbindt via een netwerk waar anderen gemakkelijk op kunnen meeluisteren (zoals een onbeveiligde draadloze verbinding) dan wordt het af luisteren van uw e-mail een risico om rekening mee te houden. Door uw e-mail via een beveiligde verbinding te versturen, voorkomt u dat uw berichten ergens op weg naar de servers van InterNLnet door derden kunnen worden gelezen. Als u wilt weten hoe u e-mail kunt versturen via een beveiligde verbinding dan leest u [hier](#) verder. Als u benieuwd bent hoe deze beveiligde verbinding werkt, dan kunt u [hier](#) verder lezen.

Het is wel belangrijk dat u zich realiseert dat deze beveiliging alleen van kracht is op het eerste deel (tot aan onze mailserver) van het traject die uw e-mailberichten afleggen naar hun ontvanger (en andersom). Vanaf onze servers vervolgt uw e-mail bericht gewoon onbeveiligd zijn weg. De beveiligde verbinding is dus vooral nuttig als u wilt e-mailen via een verbinding die u niet vertrouwt. Als u zeker wilt weten dat uw e-mail berichten slechts leesbaar zijn voor de geadresseerde, dan heeft u andere beveiligingstechnieken nodig. In dat geval raden wij u aan om meer te lezen over methodes (zoals [PGP](#) of [GPG](#)) waarmee u individuele berichten van een soort cryptografische envelop kunt voorzien.

U wilt e-mailen via een netwerk dat niet van InterNLnet is, maar u kunt onze mailservers niet bereiken

Voor mensen die veel onderweg zijn heeft beveiligd e-mailen nog een extra voordeel. Bij de gebruikelijke (onbeveiligde) manier van e-mail versturen vraagt de server die uw berichten in ontvangst neemt en voor u doorstuurt niet om een gebruikersnaam en wachtwoord. Om misbruik van dit open karakter te voorkomen, kan er alleen maar gebruik van een uitgaande mailserver (SMTP) worden gemaakt via een internetverbinding van InterNLnet. Op die manier is, in geval van misbruik (zoals het versturen van spam), de identiteit van de eigenaar van die verbinding altijd te achterhalen.

Omdat bij beveiligd e-mailen de identiteit van de verzender onomstotelijk vast staat, is deze beperking hier niet noodzakelijk. U kunt dus beveiligd e-mailen via vrijwel elke denkbare verbinding. De versleutelde verbinding loopt bovendien over een andere poort dan de standaard poort (25) voor uitgaande mail, die door veel providers naar buiten toe geblokkeerd wordt. Dit is bijzonder handig als u veel onderweg bent. U kunt overal mailen, zonder dat u de instellingen van uw e-mailprogramma hoeft aan te passen.

Hoe werkt beveiligd e-mailen?

Voor het beveiligen van de verbinding van en naar de e-mailserver maakt InterNLnet gebruik van het Secure Sockets Layer (SSL) protocol¹. Het SSL protocol is in eerste instantie ontwikkeld om communicatie (via HTTP) met normale internet pagina's te kunnen beveiligen, maar heeft zich ontwikkeld tot een van de standaarden voor beveiligde communicatie via internet. SSL heeft als voordeel dat het onafhankelijk is van het applicatie protocol. Het protocol vormt een beveiligingslaag tussen de transport protocollen (TCP/IP) van het Internet en applicatie protocollen zoals HTTP (webpagina's) of SMTP en POP3 (e-mail). Wanneer er gecommuniceerd wordt tussen server en gebruiker, zorgt SSL er door middel van cryptografie en authenticatie voor dat de data niet kan worden afgeluisterd. Zowel de authenticiteit van de zender als de ontvanger worden gecontroleerd.

SSL maakt hiervoor gebruik van een combinatie van asymmetrische en symmetrische cryptografie. Bij symmetrische cryptografie is de sleutel die gebruikt wordt om het bericht te versleutelen gelijk aan de sleutel die wordt gebruikt om het bericht te ontcijferen. Asymmetrische cryptografie werkt op basis van twee sleutels: een publieke en een niet publieke sleutel. Een bericht dat versleuteld wordt met de publieke sleutel kan alleen worden ontcijferd met behulp van de niet-publieke sleutel, en andersom. Wanneer uw e-mailprogramma verbinding maakt met een server via het SSL protocol dan stuurt deze zijn publieke sleutel terug. Met behulp van deze sleutel kan het e-mailprogramma een willekeurige geheime code versleutelen die alleen te lezen is met behulp van de niet-publieke sleutel van de server. Het SSL protocol gebruikt deze geheime code om de rest van de communicatie te versleutelen met behulp van symmetrische cryptografie. Hiermee is de vertrouwelijkheid van de verbinding met de server die de publieke sleutel af heeft gegeven gewaarborgd.

Hoe kunt u beveiligd e-mailen?

Om veilig mail te versturen en ontvangen moet u een aantal wijzigingen aanbrengen in de configuratie van uw e-mailprogramma. Hieronder wordt voor een aantal veelgebruikte e-mailprogramma's beschreven hoe u dat kunt doen. Hierbij is telkens uitgegaan van een e-mailaccount welke nog niet is ingesteld om gebruik te maken van een beveiligde verbinding. We gaan er in deze handleiding dus vanuit

¹ In bepaalde gevallen (zoals het versturen van e-mail) maakt InterNLnet gebruik van TLS, wat een is variant op, en de beoogde opvolger van, het SSL protocol.

dat uw e-mailprogramma reeds is ingesteld om op de normale, onbeveiligde manier e-mail te ontvangen en verzenden.

Microsoft outlook

Ga in de menubalk naar *Extra* en vervolgens *Accountinstellingen*. In het venster dat verschijnt (met de titel *Accountinstellingen*) kiest u het tabblad *E-mail*. Hier selecteert u uw e-mail account en vervolgens druk u op *Wijzigen*. In het venster dat verschijnt (met de titel *E-mailaccount wijzigen*) klikt u rechts onderin op *Meer instellingen*. In het venster dat nu verschijnt (met de titel *Instellingen voor internet e-mail*) kiest u het tabblad *Geavanceerd*. Het venster ziet er als volgt uit.

Instellingen voor internet-e-mail

Algemeen | Server voor uitgaande e-mail | Verbinding | **Geavanceerd**

Poortnummers van de server

Inkomende e-mail (POP3): 995 Standaardinstellingen gebruiken

Voor deze server is een versleutelde verbinding vereist (SSL)

Uitgaande e-mail (SMTP): 587

Gebruik het volgende type versleutelde verbinding: TLS

Time-outs voor de server

Kort ————— Lang 1 minuut

Bezorging

Een kopie van berichten op de server achterlaten

Van server verwijderen na 10 dagen

Van server verwijderen na verwijderen uit Verwijderde items

OK Annuleren

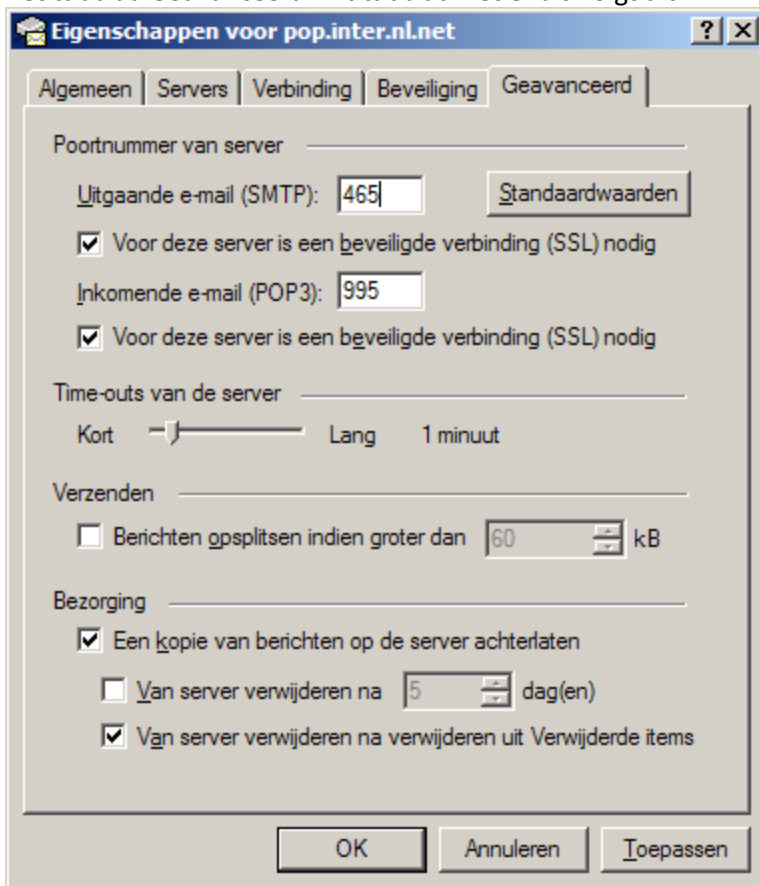
Hier vult u het volgende in:

- Inkomende e-mail (POP3): 995
- Vink het vakje aan bij *Voor deze server is een versleutelde verbinding vereist (SSL)*
- Uitgaande e-mail (SMTP): 587
- Gebruik het volgende type versleuteling: TLS

Vervolgens klikt u op *OK* om dit venster te sluiten. In het venster *E-mailaccount wijzigen* klikt u op volgende en vervolgens op voltooiën. Uw e-mail programma verstuurt e-mail in het vervolg via een beveiligde verbinding. U kunt het venster met *Accountinstellingen* sluiten om terug te keren naar Outlook.

Microsoft Outlook Express

Ga in de menubalk naar *Extra* en vervolgens *Accounts*. In het venster dat verschijnt (met de titel *Internet-accounts*) selecteert u uw InterNLnet account in de linkerkolom en vervolgens klikt u in de rechterkolom op *Eigenschappen*. In het venster dat verschijnt (met de titel *Eigenschappen voor pop.internl.net*) kiest u het tabblad *Geavanceerd*. Dit tabblad ziet er als volgt uit:

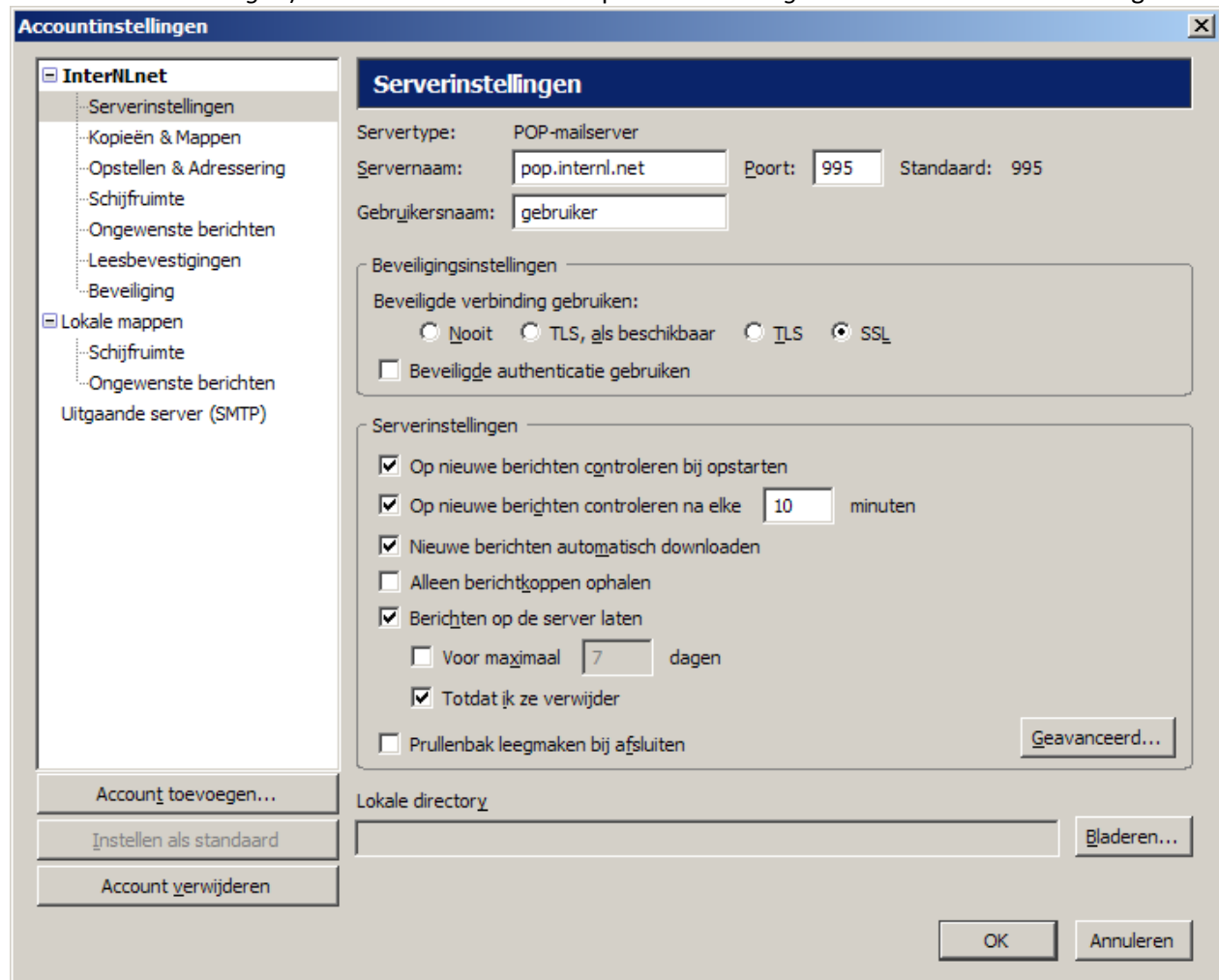


U dient hier voor zowel de uitgaande als de inkomende e-mail aan te vinken dat u gebruik wilt maken van een beveiligde verbinding. Verder vult u het volgende in:

- Uitgaande e-mail (SMTP): 465 (**let op: poortnummer wijkt af van de standaard!**)
- Inkomende e-mail (SMTP): 995

Mozilla Thunderbird

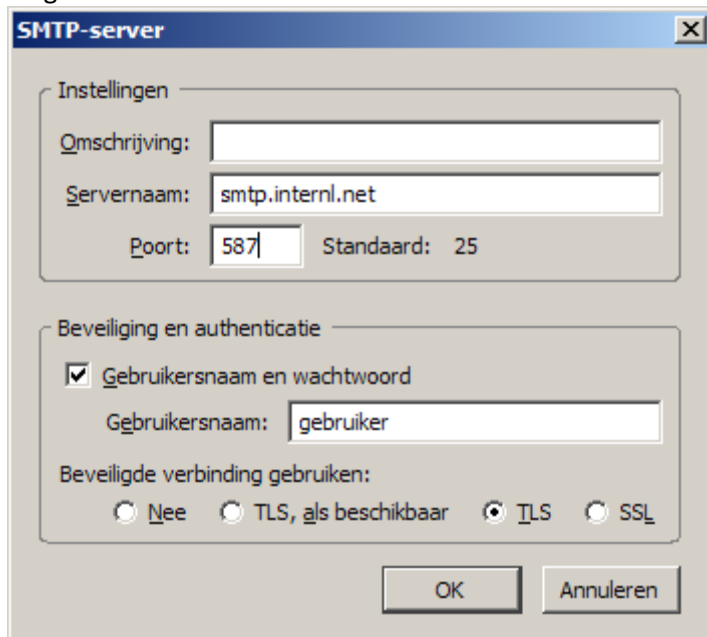
Ga in de menubalk naar *Extra* en vervolgens *Accountinstellingen*. In het venster dat verschijnt (met de titel *Accountinstellingen*) klikt u in de linkerkolom op *Serverinstellingen*. Het venster ziet er als volgt uit:



Hier vult u het volgende in:

- Servernaam: pop.internl.net
- Poort: 995
- Beveiligde verbinding gebruiken: SSL

Klik nu in de linker kolom op *Uitgaande server (SMTP)* en selecteer vervolgens in de rechterkolom uw e-mailaccount en klik op *Bewerken*. Het venster dat nu verschijnt (met de titel *SMTP-server*) ziet er als volgt uit:



Hier vult u het volgende in:

- Servernaam: smtp.internl.net
- Poort: 587
- Gebruikersnaam: uw gebruikersnaam
- Beveiligde verbinding gebruiken: TLS

Vervolgens klik u op *OK* om dit venster te sluiten. Uw e-mail programma verstuurt e-mail in het vervolg via een beveiligde verbinding. U kunt het venster met *Accountinstellingen* sluiten om terug te keren naar Thunderbird. De eerstvolgende keer dat u mail verstuurd vraagt Thunderbird om uw wachtwoord. Vul hier het wachtwoord dat bij uw e-mailaccount hoort in (en vink eventueel aan dat u dit wachtwoord wilt bewaren).