



## Technische beschrijving firewall en netwerk problemen/oplossingen met myMMX

### V1.1.a – 28/01/2014

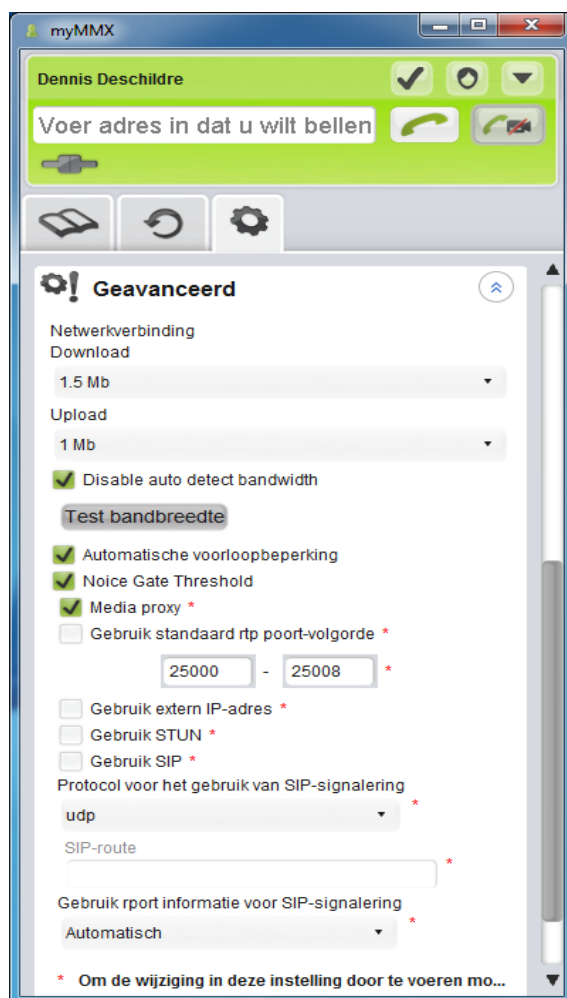
#### Introductie

Als myMMX gebruikt wordt in omgevingen met een hardware en/of software firewall, dan kunnen er problemen optreden om video/geluid te versturen/ontvangen met myMMX. Dit document beschrijft mogelijke oplossingen om dit probleem aan te pakken. Daarnaast geven we enkele referenties om aan te geven hoe dit probleem is opgelost bij verschillende bedrijven, zoals: VZW's of overheidsinstellingen.

#### Protocollen van myMMX

Als men MyMMX voor de eerste keer installeert, dan krijgt men de mogelijkheid om een aantal opties te configureren om aan te geven via welk protocol de communicatie (bij voorkeur) dient te verlopen.

De netwerkinstellingen kan men vinden door op het wielte te klikken in myMMX, dan naar het tabblad "Geavanceerd" te gaan.



Hieronder vindt men een lijst met de mogelijkheden met een korte uitleg/beschrijving.

- **Media Proxy:** deze mogelijkheid laat de communicatie van myMMX gaan langs een externe media proxy server. Deze mogelijkheid werkt zelden in firewall-omgevingen.
- **Gebruik standaard RTP poort-volgorde:** deze mogelijkheid kan men combineren met port-forwarding in de firewall. De juiste poorten voor de portforward moeten hier worden opgegeven. Deze optie moet samen gebruikt worden met “**Gebruik extern IP-adres!**”
- **Gebruik STUN:** deze mogelijkheid zorgt ervoor dat myMMX STUN (Session Traversal Utilities for NAT) gebruikt om het verkeer door de firewall te laten gaan. Werkt nooit in firewall-omgevingen.
- **Gebruik SIP:** deze mogelijkheid zorgt ervoor dat myMMX het standaard protocol voor multimedia-communicatie – genoemd SIP (Session Initiation Protocol) gebruikt. Werkt nooit in firewall-omgevingen.

**Aandacht:** als men myMMX een ander protocol laat gebruiken, dan moet men de cliënt altijd herstarten om dit protocol te laten werken.

**Troubleshooting:** als men problemen ervaart, kan men deze protocollen in volgorde uitproberen: STUN, SIP, STUN&SIP samen, RTP-port en Extern IP-adres, Media Proxy

### Portforwarding

Een eerste oplossing bestaat er in om de firewall aan te passen zodat de poorten benodigd voor myMMX worden geforward naar de desbetreffende computer.

MyMMX maakt gebruik van de volgende poorten:

- Poort 5060, zowel UDP als TCP. Wordt gebruikt voor SIP
- Poorten 25000-26000 UDP. Wordt gebruikt voor de opties “Gebruik standaard RTP poort-volgorde” samen met “Gebruik extern IP-adres”. MyMMX heeft per computer 8 poorten nodig om optimaal te werken, bvb poort 25020-25027.

Hier moet de portforward instelling er voor zorgen dat myMMX juist geconfigureerd is. We kijken even naar een oplossing die bij een organisatie in Brussel geconfigureerd is op hun firewall, en deze werkt goed.

#### Policy:

Intern	Extern	Ports	Protocol
Client IP	All	5060	TCP
Client IP	All	5060	UDP
Client IP	All	NTP	UDP
Client IP	All	25000-25020	UDP
All	Client IP	25000-25020	UDP

#### NAT filter:

Intern	Extern	Ports	Protocol
Client IP	All	25000-25020	UDP

MyMMX moet dan als volgt geconfigureerd worden (vergeet echter niet de cliënt te herstarten!):

Automatische voorloopbeperking

Noice Gate Threshold

Media proxy \*

Gebruik standaard rtp poort-volgorde \*

25000 - 25020 \*

Gebruik extern IP-adres \*

Gebruik STUN \*

Gebruik SIP \*

**Aandacht:** uit ervaring is bekend dat deze poorten forwarden naar een IP-range i.p.v. een specifiek IP-adres niet

zal werken. Bij een gebruiker in Gent is eerst geprobeerd deze poorten te forwarden naar een IP-range – dit werkte niet. Daarna is besloten (na technisch overleg) om deze poorten te forwarden naar een specifiek IP-adres, met als resultaat: myMMX werkte goed en zowel geluid/beeld kwamen goed door de firewall.

Indien de voorgaande oplossing niet zou werken, dan kan er geopteerd worden voor een andere aanpak om de firewall aan te passen: zorg ervoor dat het bepaalde IP-adres van de computer waarop myMMX geïnstalleerd is, totaal geen restricties heeft in de firewall.

Feitelijk dient de firewall geconfigureerd te worden zodat het bepaalde IP-adres volledige toegang heeft tot internet. Dit kan wel security issues veroorzaken.

Daarom is het aangewezen om ook eens kijken naar de onderstaande optie om een firewall te bypassen.

### **Bypass van firewall**

Een tweede mogelijkheid is om de computer via een externe lijn rechtstreeks met het internet te verbinden om zo de firewall te omzeilen. Concreet genomen kunnen we hier 2 opties onderscheiden:

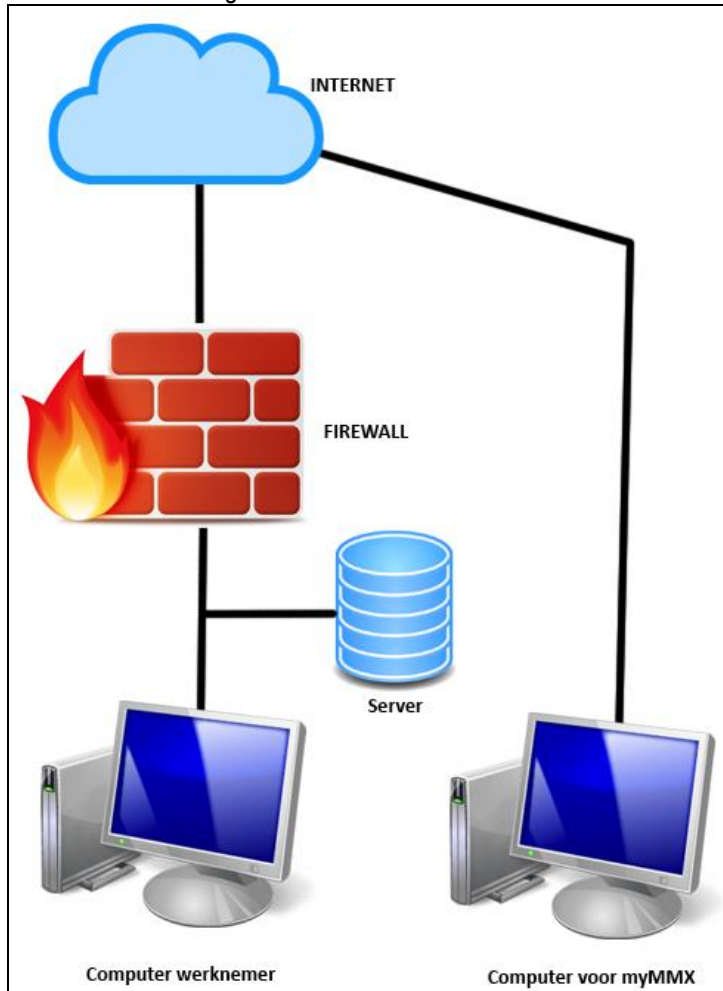
**Optie 1:** een extra computer of laptop met webcam voorzien voor de dove werknemer, en deze aansluiten op een externe lijn zodat myMMX gebruikt kan worden.

Voordelen: de huidige computer (computer werknemer in grafische voorstelling) blijft aangesloten “achter” de firewall en een verbinding met de eigen servers (mail, data,...) blijft behouden zodat alles gewoon eigenlijk bij het oude blijft.

Het verschil is dat men een extra computer voorziet voor de dove werknemer samen met een externe/extra lijn naar het internet. Het maakt niet uit wat voor lijn het is of welke toestellen (firewalls, routers) er tussen zitten maar zolang myMMX goed werkt op deze lijn, is het ok.

Nadelen: er is een kleine investering nodig voor een tweede computer of laptop met webcam, en er moet een externe lijn worden aangelegd rechtstreeks naar het bureau van de dove werknemer.

Grafische voorstelling:



Deze oplossing wordt vooral toegepast bij gebouwen van de Vlaamse Overheid waar de computers zo streng beveiligd zijn dat het niet mogelijk is om myMMX uit te voeren op de PC zelf. Voor de dove werknemers wordt er dan een 2e laptop voorzien die via het “VO-bezoeker” WiFi-netwerk verloopt! Deze laptop moet een standaard Windows operating system hebben, geen VO-build. Ter info: op alle computers/laptops van de Vlaamse Overheid wordt er een aangepast Windows operating system – de VO-build – geïnstalleerd waarmee men deze in het VO-netwerk kan gebruiken.

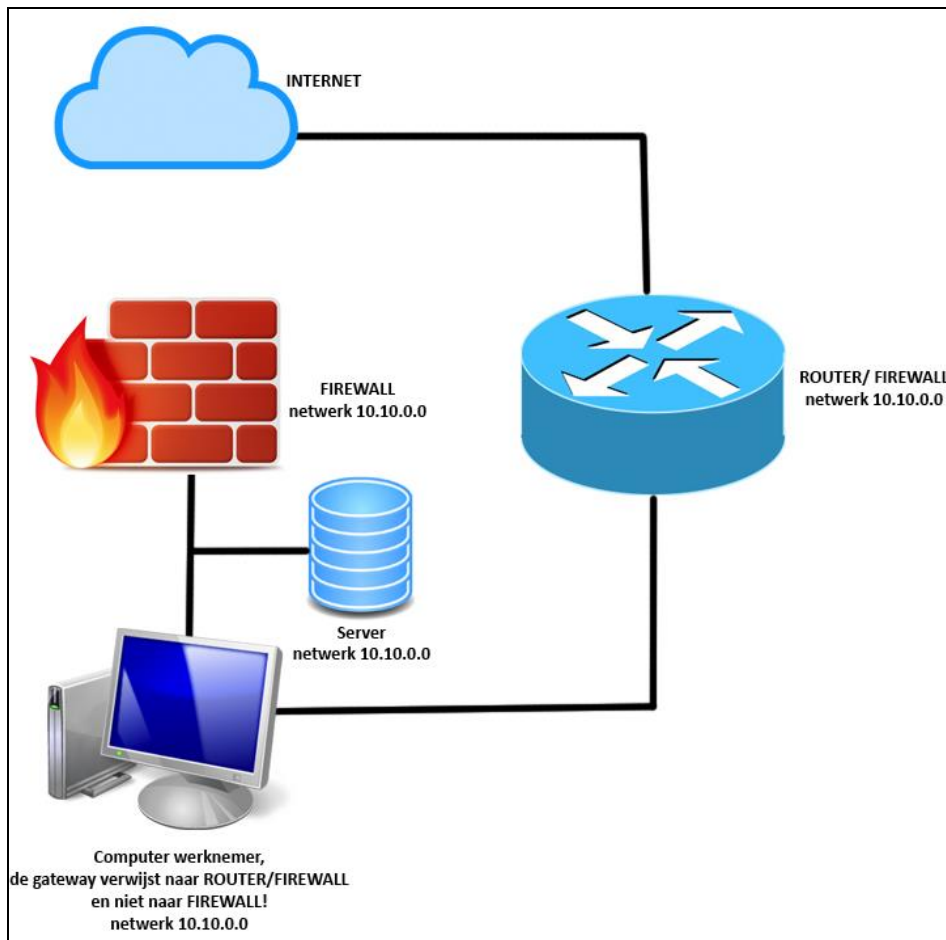
**Optie 2:** men laat het internetverkeer van de computer verlopen via een andere router/firewall die in hetzelfde netwerk zit, maar toelaat dat myMMX kan communiceren naar buiten toe.

Deze oplossing is gelijkaardig aan de vorige, maar het enige verschil is dat er geen 2e toestel wordt voorzien aangezien men het internetverkeer van de PC laat lopen via een andere router/firewall dan de huidige bestaande firewall. Deze router/firewall laat myMMX toe om te communiceren met internet en zo goed beeld/video te ontvangen. Hoe doet men dit? Men configureert het IP-adres van de computer handmatig en als gateway gebruikt men de router/firewall die geen restricties geeft aan myMMX.

Voordelen: de huidige computer blijft in het netwerk zitten en zal altijd verbonden zijn met de eigen servers (mail, data,...).

Nadelen: er moet een router/firewall worden aangekocht en geïnstalleerd in hetzelfde netwerk. Bij voorkeur moet dit een router/firewall zijn die standaard het SIP-protocol ondersteunt.

Grafische voorstelling:



Deze oplossing wordt toegepast bij een onderneming in Gent. Er is hiervoor een Intertex IX78 aangekocht en geïnstalleerd. Al de computers hier hebben het SIP protocol geconfigureerd met TCP protocol en route voor SIP-signalering.

### Bandbreedte

Om myMMX optimaal te laten werken is er een minimale bandbreedte van 1,5Mbs/s download en 1Mb/s upload benodigd.