

Community thuisgebruik via Internet

Technische gegevens en instellingen beeldbellen

VieDome Community maakt gebruik van open internet via de eigen internetverbinding van de klant. Voor thuisgebruik wordt internet aangeboden door vele leveranciers en deze leveranciers gebruiken hiervoor een scala aan verschillende typen routers en andere apparatuur. Met overgrote deel van deze apparaten kan VieDomeCommunity probleemloos gebruikt worden. Bij sommige apparaten is een extra handeling nodig. Deze folder vertelt u hier meer over.



Er zijn veel verschillende soorten routers te krijgen, maar de manier waarop die routers omgaan met toegangsbeveiliging tot het netwerk waar ze als gateway dienen, is wat voor ViedomeCommunity vooral van belang is. Hierin zijn 4 types te onderscheiden:

Full cone, of één op één NAT (network address translation) traversal, waarbij een programma van het intranet (het thuis netwerk) de router aangeeft dat verkeer op een bepaalde poort op de router doorgestuurd mag worden naar dit programma.

Address restricted cone, waarbij een programma vanuit het intranet aangeeft verkeer te willen ontvangen van een partij op het internet, door naar het adres (IP adres) van deze partij een netwerk pakket te sturen. Dit resulteert in een vaste poort op de router voor alle berichten vanuit dit programma. Alle berichten die vervolgens naar deze poort worden gestuurd vanuit de externe partij worden door gestuurd naar het programma op het intranet.

Port restricted cone, waarbij een programma vanuit het intranet aangeeft verkeer te willen ontvangen van een partij op het internet, door naar het adres (IP adres) en een specifieke poort van deze partij een netwerk pakket te sturen. Dit resulteert in een vaste poort op de router voor alle berichten vanuit dit programma. Alle berichten die vervolgens naar deze poort worden gestuurd vanuit de externe partij en vanuit de poort waar het eerste bericht heen was gestuurd, worden door gestuurd naar het programma op het intranet.

Symmetric NAT, waarbij een programma voor elk verkeer naar een andere externe partij een nieuwe poort op de router krijgt toegewezen. Alleen berichten die vanuit deze externe partij terugkomen op dezelfde poort op de router worden doorgestuurd naar het programma.

Het probleem is nu dat van te voren niet na te gaan is welke poort gebruikt zal gaan worden op de router voor berichten naar een externe partij. Om dit te achterhalen wordt door ViedomeCommunity gebruik gemaakt van een centrale server, die kan detecteren waar pakketten precies vandaan komen, en dat vervolgens reflecteert. Alleen in geval van een symmetrische NAT heeft dat geen zin, want de poort die gebruikt wordt naar de centrale server zal niet hetzelfde zijn als de poort die naar de uiteindelijke externe partij gebruikt wordt. Videoverbindingen vanuit een symmetrische NAT naar een andere symmetrische NAT of naar een port restricted cone NAT zullen daarom mislukken: verkeer wat van een verkeerde poort komt wordt niet doorgegeven naar het programma. De overige twee zullen pakketten vanuit een symmetric NAT wel door sturen naar het programma, ook al kloppen de poorten niet, en aan de hand van deze pakketten zal het programma detecteren wat de echte poort is die gebruikt moet worden bij de tegenpartij.

Nu is er een alternatief voor deze NAT traversal strategie, namelijk UPnP (Universal Plug and Play). Dit is een internationale afspraak (standaard) voor apparaten die aangesloten zijn op een netwerk, zoals bijvoorbeeld netwerk printers, routers of media servers. Via een vastgelegd recept van berichten kunnen deze worden gedetecteerd in een intranet (het thuis netwerk). Daarnaast moet elk type apparaat een aantal standaard functies ondersteunen. Bij routers is dat onder andere de mogelijkheid om vanuit het intranet een poort te reserveren voor verkeer van en naar een specifiek apparaat binnen het intranet (poort forwarding). Men mag er dus vanuit gaan dat als UPnP wordt ondersteund door een router, deze functie beschikbaar is, en ook goed functioneert.

Alle routers van KPN die tot nu toe zijn getest zijn van het type symmetric router. De router bij Mextal (en bij VM) is een Port restricted cone router. Stephane heeft thuis een Address restricted cone, vandaar dat hij altijd van thuis uit een verbinding op kan zetten naar een symmetric router, zonder verdere maatregelen te nemen.

Helaas geeft de door KPN gebruikte Siemens Gigaset SX551 aan wel UPnP te ondersteunen, maar blijkt vervolgens bij de aanroep van de functies om poort forwarding te reserveren te antwoorden met 'niet geïmplementeerd'. Een verbinding opzetten zal dus niet gaan lukken naar een andere symmetric router of een port restricted router! KPN geeft aan dat er inderdaad problemen zijn met UPnP, maar dat deze router end of live is, en niet meer wordt uitgeleverd. Nieuwe aansluitingen zullen deze router ook niet meer krijgen, maar vervanging vindt pas plaats als gebruikers daadwerkelijk problemen ondervinden in normaal internet gebruik.

De uiteindelijke oplossing voor dit type router (en eventueel andere symmetric routers die geen UPnP ondersteunen) is om naast het NAT traversal algoritme ook een relay methode (TURN) te ondersteunen. Hiermee wordt verkeer als laatste resort naar de centrale server gestuurd, die ook gebruikt werd om de externe poort op de router te detecteren. Deze route blijft geldig, ook bij een symmetric router. De server op zijn beurt zal het verkeer vervolgens door sturen naar de externe partij op het internet. Bijkomend voordeel is wel dat dit eventueel ook te gebruiken is als 'multicaster', waardoor one to many verbindingen mogelijk worden: video en audio wordt vanuit één punt naar de server gestuurd, en deze stuurt het naar meer ontvangende partijen. Nadelen zijn de extra vertraging die wordt opgelopen doordat het verkeer altijd eerst naar de centrale server moet, en een behoorlijke impact op de netwerk en CPU load van deze centrale server.

Conclusie

Om kort te gaan, uitgaande van de bestaande type routers voor thuis gebruik is de mogelijkheid om succesvol een verbinding op te zetten in een matrix te vangen (van = verticaal, naar = horizontaal):

Router type	I	Full Cone	Address restricted	Port restricted	Symmetric
I	✓	✓	✓	✓	✓
Full Cone	✓	✓	✓	✓	✓
Address restricted	✓	✓	✓	✓	✓
Port restricted	✓	✓	✓	✓	✗
Symmetric	✓	✓	✓	✗	✗

I : Rechtstreeks aan het internet, geen router aanwezig

Dus, vanuit 25 mogelijke combinaties zijn er drie die problemen kunnen geven.

De eerste oplossing: in die gevallen is UPnP, waarmee vanuit het programma (de plugin) poort forwarding kan worden aangezet, waardoor deze router zich gedraagt als een full cone router: alle berichten op de opengezette poort worden doorgestuurd naar het programma die dit heeft aangevraagd.

De tweede oplossing: mocht UPnP niet worden ondersteund, of niet correct zijn geïmplementeerd, is er tenslotte nog de mogelijkheid om de audio en video via een speciale relay server te versturen (*is Q3 2011 gereed*).

Bedrijfsnetwerken en publieke netwerken in bijv. hotels voegen vaak nog een extra niveau aan beveiliging toe, en blokkeren in principe alle verkeer wat ze niet expliciet toestaan. Met behulp van de systeembeheerders is ook in deze situaties beeldbellen altijd mogelijk. (*Zie de folder technische specificatie beeldbellen via bedrijfsnetwerken*)

Aan deze folder kunnen geen rechten worden ontleend. Mextal behoudt zich het recht voor de configuratie te wijzigen.