ZeroTier

EEN PLANEETOVERSTIJGENDE VIRTUELE SWITCH

We hebben steeds meer apparaten en servers in huis, die allerlei taken vervullen en die we kunnen bedienen zolang we met hetzelfde netwerk verbonden zijn. We vinden het tenslotte niet zo'n goed idee als Jan en alleman op onze homeserver door onze vakantiefoto's kan struinen of onze lampen aan- en uit kan zetten. **Martin van Es**

Om deze servers, die we op afstand willen onderhouden, toch bereikbaar te maken van buitenaf kunnen we een SSH daemon installeren en een poortje openen aan de buitenkant. De server moet dan wel een statisch IP-adres in de private range aan de binnenkant hebben. Om het veiliger te maken kunnen we een VPN-oplossing installeren en ons zo toegang verschaffen tot het lokale netwerk thuis. Maar het kan ook een stuk simpeler met ZeroTier.

ZeroTier is een open source Software Defined Network dat op basis van huis-tuin-en-keuken IP-verbindingen een beveiligde laag en peer-to-peer netwerk verzorgt. Bovenaan de ontwerpcriteria stonden gebruiksgemak, veiligheid en decentralisatie. Dat die drie niet hand in hand gaan, is te lezen in het manifest dat Adam Ierymenko op 1 augustus 2014 publiceerde toen hij voor het eerst over ZeroTier aan het nadenken was (zie referenties [1]).

MOTIVATIE

In 2014 schrijft Adam Ierymenko een blog over een idee dat hij ZeroTier noemt, waarin hij beschrijft waar een gebruiksvriendelijk en veilig peer-to-peer VPN volgens hem aan moet voldoen. Zijn conclusie is dat gebruiksvriendelijkheid en volledige decentralisatie elkaar uitsluiten. Een belangrijke (technische) reden hiervoor is dat een peer-to-peer netwerk, waarin peers zich achter NAT-verbindingen verschuilen, het moeilijk maakt elkaar te vinden zonder een hulpje van buitenaf. Deze hulp vormt het zogenaamde centrale punt en de achilleshiel van het verlangen volledig decentraal en onafhankelijk te zijn.

Uiteindelijk kiest Adam voor een compromis, waarin een aantal domme en blinde centrale servers de peer-to-peer connecties tot stand helpen brengen, zonder dat deze inzage hebben in de communicatie of deze kunnen manipuleren. Deze zogenaamde Root servers zijn te vergelijken met de DNS root servers en helpen bij het opzetten van de peer-to-peer connecties. Dit werkt net zoals de DNS root servers je doorverwijzen naar de verantwoordelijke DNS-server voor het domein waar je naar op zoek bent. Alleen als er écht geen rechtstreekse verbinding mogelijk is, blijven de Root servers betrokken bij de communicatie, waarbij ze volledig blind zijn voor de inhoud van de pakketten.
De ZeroTier client zal eerst proberen