Interview | Hans Steeman

Dedicated oplossingen voor een veilige infrastructuur

A10 Networks brengt hyperscale-beveiliging tegen cyberaanvallen naar 5G-infrastructuur

Veiligheid voor netwerken is de grootste kopzorg van veel CIO's en IT-beheerders. Hoe houd je alle ellende buiten de deur? Op Mobile World Congres spraken wij met Paul Nicholson, senior director of Product Marketing bij A10 Networks, en Ronald Sens, directeur EMEA Marketing bij A10 Networks. Deze gerenommeerde fabrikant is een specialist op het gebied van netwerkbeveiliging met een hoofdzetel in het Amerikaanse San Jose (Californië).

A10 Networks is een speler van formaat met klanten in meer dan tachtig landen. Het zijn afnemers die gebruikmaken van het pakket van applicaties en diensten om cybercrime onder controle te houden. A10 Networks is gebouwd op de fundamenten van Foundry Networks, indertijd een specialist op het gebied van routers en switches. Zowel Japan als de USA zijn de elementaire thuismarkten. Veel grote enterprises en serviceproviders maken daar al sinds 2006 gebruik van de A10 load balancers.

A10 Networks verdeelt zijn activiteiten over drie aandachtsgebieden: multi-cloud application deliverysystemen, DDoS-protectiesystemen en sinds kort de 5G-infrastructuur van telecomproviders. Dit laatste cluster is zeer interessant, omdat daar een grote consolidatie van technologieën plaatsvindt en het een groeimarkt van formaat is. De Gi-firewall, de traffic steering en de load balancing zijn bij A10 in goede handen. Paul Nicholson: "Onze kennis is ontstaan in de hardware-industrie en de ruime ervaring betaalt zich nu uit. De Gi-firewall is een instituut op zichzelf en bewijst ook nu zijn toegevoegd waarde." Bijna alle producten gaan naar de markt via het resellerkanaal, Paul Nicholson schat dat 95 procent van de sales via de channelpartners gaat.

Tijdens Mobile World Congres was er veel aandacht voor de bedreigingen van de mobiele 5G-netwerken, die dankzij hun uitgebreide range aan toegangspunten waarmee verbinding met het internet gemaakt wordt, extra aandacht vereisen inzake de veiligheid van het netwerk. Ronald Sens, directeur EMEA Marketing bij A10 Networks: "Met de introductie van 5G-netwerken komt IoT in een stroomversnelling. Steeds meer sensoren worden via dat netwerk aangesloten. Het aantal ingress-punten neemt exponentieel toe, een reden om hier veel aandacht aan te schenken". Meer en meer apparaten online en steeds grotere data-stromen zijn het resultaat van deze ontwikkeling.

Internet wordt steeds verder gepene-treerd met cybercriminaliteit. Voor de hackers wordt het steeds eenvoudiger doordat complete toolkits voor deze activiteiten te downloaden zijn. Het realiseren van een DDoS-aanval is dan kinderspel. Een gemiddeld huishouden heeft binnenkort zo'n 30 connected IoT-devices, dat creëert een grote uitdaging voor beveiligers. Doordat de technologie zo eenvoudig is en breed verspreid, lukt het niet langer om op basis van vingerafdrukken malware te onderscheppen. De vingerafdrukken veranderen continu waardoor een database niet bij te houden is. Het is het gedrag van code dat verraadt dat er iets vreemds speelt. Beveiligers proberen dat beter onder controle te krijgen. Daar zijn veel geavanceerdere configuraties voor nodig, aldus Ronald Sens. Precies dát is bij A10 Networks in uitstekende en betrouwbare handen.

www.a10networks.com | emea@a10networks.com | 020 218 1288