



ICT CENTRAAL IN NEDERLAND

# EEN BALANS TUSSEN 5G EN BESTAANDE NETWERKEN

**Anthony Webb**  
VP EMEA A10 Networks

**De eisen aan netwerken worden steeds strenger. Het valt te verwachten dat de markt flinke ontwikkelingen doormaakt. Ook A10 Networks ziet veel gebeuren, maar verwacht vooral dat de balans moet gevonden tussen de anticipatie op 5G en het beheer van bestaande netwerken. Anthony Webb, VP EMEA bij A10, licht het toe.**

Tekst Michiel van Blommestein

Voor veel organisaties zijn netwerken een gegeven. Ze doen het of ze doen het niet en als ze het niet doen is het vaak ook meteen een enorm probleem. Niemand lijkt na te willen denken over hoe ze hun netwerken in de lucht moeten houden of ze uitbouwen voor eventuele nieuwe behoeften. “En zo hoort het te zijn”, zegt Webb. “Maar voor de engineers wordt het komende jaar zeer interessant”, voegt hij eraan toe. Meteen noemt Webb de belangrijkste ontwikkeling die de markt het komende jaar gaat vormen: 5G.

## Nieuwe investeringen

De anticipatie van 5G zal naar verwachting komend jaar in een stroomversnelling raken, en dat zullen we zien in de investeringen die leveranciers gaan doen. De techniek is er en werkt, terwijl onderhand de normen worden omschreven. Webb verwacht dat we in 2019 ook de eerste product-roadmaps gaan zien. “Onze pilotprojecten hebben al

enkele uitdagingen voor serviceproviders blootgelegd”, zegt Webb. “De eisen van 5G zijn anders dan die van 4G. De packets zijn kleiner met snellere doorgifte en meerdere verbindingen tegelijk. Het is aan de serviceproviders om soms wel miljarden sessies tegelijk

**‘Cybercriminelen slagen er steeds beter in om binnen te komen, dus de aandacht gaat uit naar het snel identificeren en elimineren van dreigingen’**

door te geven en hogere capaciteit te bieden.” Maar, zo zegt Webb, de beveiliging van de infrastructuur is zo mogelijk een nog veel groter vraagstuk. “Het moet allemaal worden gemoderniseerd, met automatisering en schaalbaarheid ingebouwd om de uptime te garanderen en de beveiliging aan zowel de beheerders- als de

gebruikerskant.” Dat betekent dat firewalls en DNS-bescherming moeten meegaan met de 5G-ontwikkelingen. “We gaan ook sterke verbeteringen zien in kunstmatige intelligentie en machine learning zodat security-oplossingen een antwoord hebben op DDoS-aanvallen.

Met Internet of Things hebben criminelen meer mogelijkheden voor dat soort aanvallen.” Volgens Webb kan 5G alleen een succes worden als de latency en TCO laag blijven. “De concurrentie in deze markt zal enorm zijn”, zegt hij. “Leveranciers zullen dus flink investeren in hun technologie zodat hun netwerken er klaar voor zijn.”

## Behoud van bestaande netwerken

Maar de uitrol van 5G gaat niet over één nacht ijs. Serviceproviders hebben veel geïnvesteerd in hun bestaande netwerken die ze niet zomaar kunnen afschrijven. Meer investeringen in wat eigenlijk snel achterhaald is dus? Op zich is dit echter helemaal niet zo vreemd, zo denkt Webb. Upgrades zijn duur, dus kiest men liever voor een verbetering aan wat er al ligt. “Neem de IP-adressen. De voorraad van IPv4-adressen raakt snel op, vooral door al die IoT-apparaten”, zegt hij. “De verwachting was dat iedereen uiteindelijk overstapt naar IPv6 om het probleem op te lossen. Maar dat is eigenlijk een volledige upgrade, en dienstverleners kiezen daar niet zomaar voor. In plaats daarvan implementeren ze technologie als Carrier Grade Networking (CGN) om hun investering mee te borgen. Ze halen dan het beste uit hun bestaande technologie en verlengen de levensduur, terwijl ze geleidelijk plannen maken voor een overgang naar IPv6.” Webb denkt dat de overgang naar 5G vergelijkbaar zal zijn. “Alles in één keer vervangen is gewoon te duur.”

Webb pakt de security er weer bij, want behalve dat de technologie grote sprongen zal maken, vermoedt hij ook dat de algemene aanpak in de kern zal veranderen. “De filosofie is volwassener”, zegt hij. “De mentaliteit waarbij we een barrière om het netwerk opwerpen en deze met hand en tand verdedigen, maakt plaats voor een pragmatische aanpak.” Steeds meer professionals worden er zich van bewust dat het dichttimmeren van de omgeving een verloren zaak is. “Cybercriminelen slagen er steeds beter in om binnen te komen, dus de aandacht gaat uit naar het snel identificeren en elimineren van dreigingen.” DDoS blijft een groot risico, vooral omdat dergelijke aanvallen steeds eenvoudiger zijn om uit te voeren. “Bescherming tegen DDoS is domweg broodnodig geworden”, zegt Webb. “En daarvoor heb je geautomatiseerde, slimme en schaalbare bescherming nodig, ook nog eens tegen een lagere TCO.”

## Een ander businessmodel

De laatste jaren is ICT-breed de voorkeur voor operationele kosten boven investeringskosten naar het eerste doorgeslagen. “Organisaties wilden altijd hun CAPEX verlagen en een iets hogere OPEX op de koop toenemen”, zegt Webb. “Maar als er een grote upgrade aankomt, dan weet je dat die aanpak je technologisch op achterstand gaat zetten die je uiteindelijk moet inhalen. Dat is een risico waar veel serviceproviders vraagtekens bij zetten.” Hij verwacht dan ook dat zij het komende jaar meer

aan de lange termijn gaan denken. “Ze gaan denk ik iets meer vooruit betalen om de operationele kosten op langere termijn iets te drukken.”

Hoe dan ook verwacht Webb een bewogen jaar voor netwerkleveranciers en hun partners. “Ik verwacht dat we branche-breed naar een balans gaan zoeken tussen de invoering van 5G en het behoud en onderhoud van bestaande netwerken”, zegt hij. “Tegelijkertijd moeten we ons storten op de beveiliging. Het zal zeker geen saai jaar zijn.” «



Anthony Webb