Barracuda

Microsoft

4 scenario’s voor een veilige migratie naar de cloud

De cloud lijkt het toverwoord voor een flexibelere bedrijfsvoering en hogere rendementen. Daarom willen steeds meer organisaties naar de cloud migreren. Hoe gaat dat op een veilige manier en hoe zorg je dat de verbinding met de public cloud en de apps die daar staan veilig zijn? We beschrijven vier scenario's uit de praktijk.

Niet elke organisatie is hetzelfde. Daarom kent elke organisatie zijn schaal der geleidelijkheid om naar de cloud te gaan. Op dit moment zien veel bedrijven het als hét moment om (geleidelijk) afscheid te nemen van hun eigen on-premise datacentrum. Dat doen ze vanwege een aantal voordelen die cloud computing biedt. In de klassieke benadering kocht je het nieuwste, grootste en snelste wat er op dat moment in de markt te krijgen was om die ene piek op te vangen voor je on-premise datacenter. Dat hoeft niet meer omdat je in de cloud betaalt naar gebruik.

Je betaalt in de cloud wat je echt nodig hebt en dat is snel op afstand op te schalen of uit te zetten. Welke IOPS zijn noodzakelijk en welke bandbreedte is vereist? Wat moet wel, niet of slechts zo nu en dan gemirrord worden? Wat is het schema van minimale en maximale belasting? Moet de service zeven dagen per week beschikbaar zijn op maximale capaciteit? Of hoeft dat alleen tijdens kantoortijden of zelfs maar een paar uur per maand of per week als de rekeningen worden opgemaakt? Hierdoor kunnen services op sommige tijden wel helemaal uit. Diensten op de servers stonden aan en bleven aan, of ze aangesproken werden of niet. Dat kost samen met de afschrijving van de hardware enorm veel geld. In een on-premise datacenter moet er bij vergroting van opslag of rekenkracht fysiek worden bijgeplaatst. Maar dat hoeft niet meer omdat op afstand met een slider direct kan worden opgeschaald. Bezit en beheer is iets uit het verleden omdat de hardware, de infrastructuur en de software als abonnement wordt afgenomen.

Dat klinkt voor veel organisaties iets van nabije toekomst. Als je een eigen, modern datacenter hebt, is het afschrijven ervan misschien nog helemaal niet zo handig. Daarnaast zijn er bepaalde legacy applicaties die (nog) niet geschikt zijn gemaakt voor het ecosysteem van de cloud. Het kan ook zijn dat je liever grip houdt op bepaalde services. Aan de andere kant zie je dat oplossingen juist beter vandaag dan morgen naar de cloud gemigreerd kunnen worden. Bijvoorbeeld omdat flexibiliteit- en schaalbaarheidsvoordelen van de cloud de business een stuk wendbaarder maakt.

Extra security en inzicht in data in de cloud

De dataveiligheid op Azure is van enterprise-niveau en wordt continu verbeterd. Hierdoor zijn onder andere persoonsgegevens compliant aan wet- en regelgeving op te slaan. Tegenwoordig kan worden gekozen om clouddata binnen het grondgebied van de EU op te slaan. Hierdoor blijft privacygevoelige informatie ook binnen Europese regelgeving.

De keuzevrijheid zit niet alleen in de mate van beveiliging. Microsoft Azure is een open cloud. Het is bijvoorbeeld geen enkel probleem om Linux-servers op het platform te draaien. Dat geldt ook voor andere software als third party apps en extra security. Zo beveiligen de firewalls van Barracuda verbindingen, zorgen ze voor continuïteit en, houden ze toezicht op authenticatie. Daarnaast beveiligen ze applicaties van derden op Azure en vergroten ze de beveiligingsmogelijkheden van deze clouddienst. Niet voor niets maken marktleiders op het gebied van energie, levensmiddelen en gezondheidszorg gebruik van Azure in combinatie met Barracuda. Je kunt het zien als een extra bumper en extra sensoren die je voor je auto koopt zodat die minder snel een deuk oploopt. Door gebruik te maken van de Web Application Firewalls (WAF) en de NextGen Firewall (NGF) krijg je nóg meer grip op de security van de applicaties op Azure en de datastroom van en naar de cloud. Dat is in sommige gevallen namelijk gewenst.

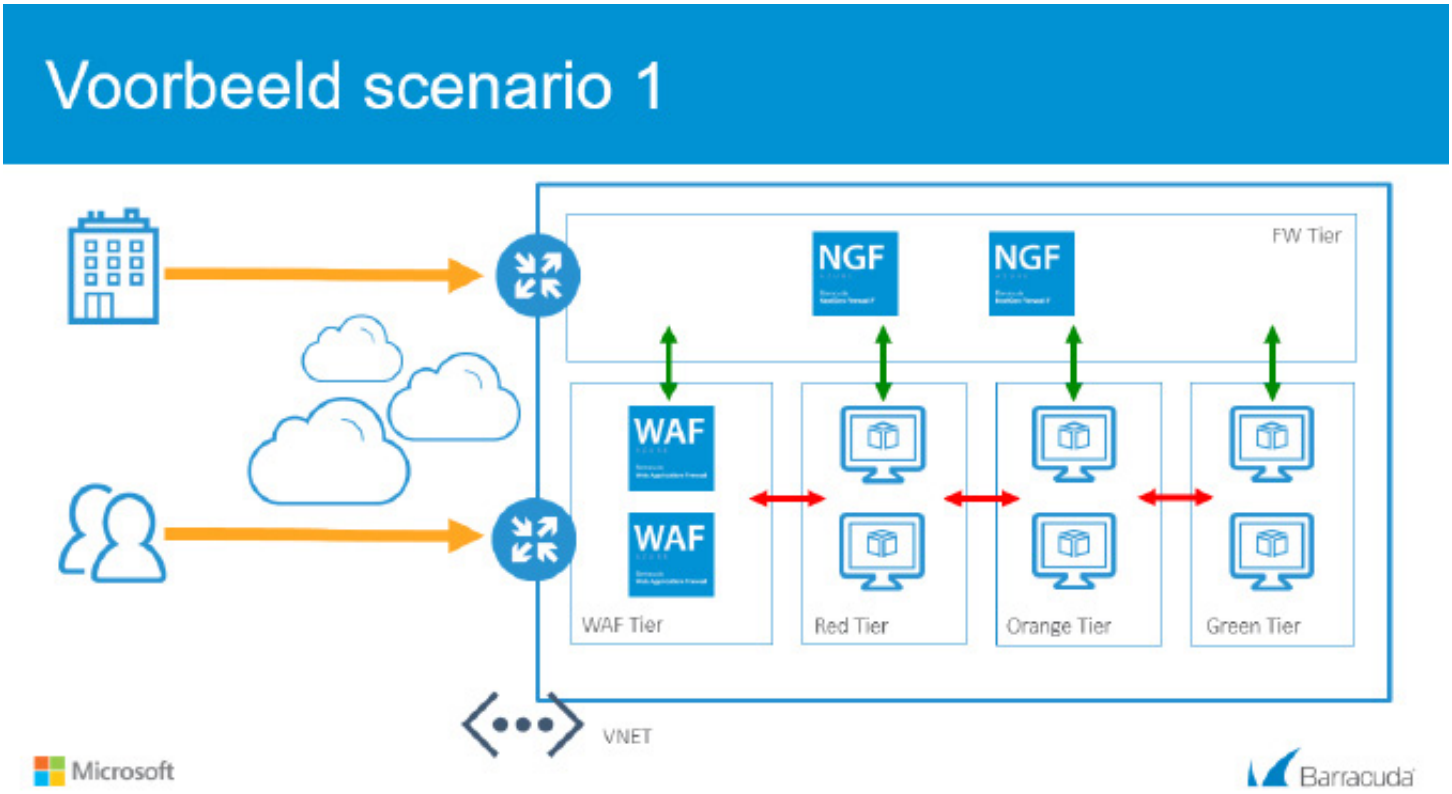
Een on-premise datacenter werkt namelijk net even anders dan het cloudplatform Azure. Microsoft beschermt wel de eigen applicaties op deze clouddienst, maar niet de applicaties die bedrijven er zelf op zetten. Als je een applicatie naar Azure migreert, verzorgt Barracuda de beveiliging ervan. Dat geldt ook voor authenticatie. Zo checkt Barracuda of de ontwikkelaar bijvoorbeeld wel de juiste rechten heeft om op het ontwikkelplatform te werken. Op die manier wordt de verbinding tussen lokaal en Azure beveiligd. Met Barracuda kan er een Demilitarized Zone (DMZ) gebouwd worden waarmee meerdere subnets binnen een Azure VNET gemaakt kunnen worden. Hiermee krijg je volledige controle op logins en het geeft inzicht welk verkeer er in en uit gaat.

Bij een migratie naar Azure mis je overzicht in dataverkeer dat je on-premise wel had. Dit inzicht is wel handig om prioriteit aan applicaties te kunnen geven. Als bijvoorbeeld op een dag door medewerkers veel naar YouTube wordt gekeken, kunnen collega's bijvoorbeeld niet goed Skypen omdat de bandbreedte niet meer toereikend is. Daarom is het handig dat de firewall van Barracuda bijhoudt wat bedrijfskritische data is of niet. Een grote Nederlandse zorgverzekeraar verhuisde onlangs zijn datacenter naar Azure en migreerde SharePoint ook mee. De prioriteit van deze applicatie moest natuurlijk zo hoog mogelijk zijn zodat er altijd mee gewerkt kan worden. De connectiviteits-gateway (firewall) van Barracuda zorgt ervoor dat het verkeer voor deze applicatie en bijvoorbeeld Skype voor Bedrijven altijd voorrang krijgen.

Het is allereerst de vraag welke onderdelen van de organisatie je verhuist. Dat lees je in het vorige deel in deze serie over migratie naar de cloud Welke toepassingen migreer je wel of juist niet naar de cloud?. De volgende stap is hoe je dat op een veilige manier doet.
Hiervoor nemen we vier scenario's onder de loep.

Scenario 1: de volledige IT-omgeving migreren naar de public cloud

De coöperatie van boeren en tuinders Agrifirm zag dat ze met meerdere diensten van Azure een modernere organisatie konden worden. Ze wilden toegang tot verschillende zones van het systeem met verschillende risiconiveaus. In hun business case komen de gebruikers zowel van binnen als buiten het bedrijfsnetwerk. Zij wilden daarom centrale controle op wie en wanneer er wordt ingelogd. Daarom is er een NGF ingezet om de communicatie van het hoofdkantoor te beveiligen. Daarnaast is een WAF ingezet om apps op Azure te beveiligen en een NGF om de verschillende zones te creëren.

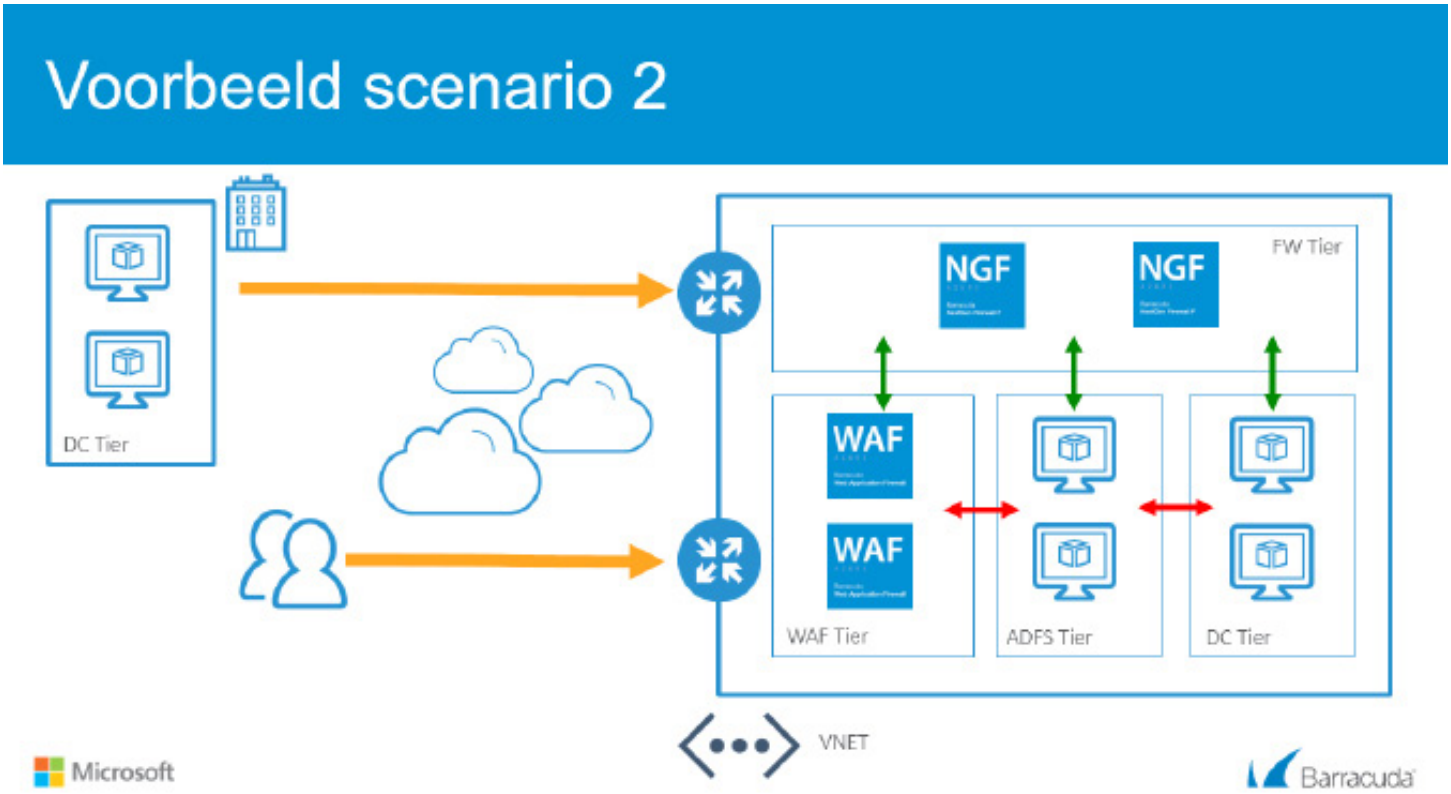


Figuur 1

In Figuur 1 zie je dat links bovenin het verkeer vanuit het hoofdkantoor naar Azure gaat. De logins worden door de NGF gescreend of ze toegang mogen krijgen en hoe diep in het systeem. In het figuur linksonderaan zie je de mobiele gebruikers die inloggen op het systeem via de WAF binnenkomen. Wie is het, welke rechten hebben ze en moeten ze nog door de NGF? Op die manier worden de moderne beveiligingsuitdagingen getackeld. Deze oplossing wordt nu gebruikt en we zien dat steeds vaker remote wordt ingelogd. Dankzij het vertrouwen in deze oplossing, worden medewerkers van Agrifirm mobieler. Ze hoeven immers niet meer naar het hoofdkantoor om bij de goed beveiligde bedrijfsinformatie te kunnen. datacenter hebt, is het afschrijven ervan misschien nog helemaal niet zo handig. Daarnaast zijn er bepaalde legacy applicaties die (nog) niet geschikt zijn gemaakt voor het ecosysteem van de cloud. Het kan ook zijn dat je liever grip houdt op bepaalde services. Aan de andere kant zie je dat oplossingen juist beter vandaag dan morgen naar de cloud gemigreerd kunnen worden. Bijvoorbeeld omdat flexibiliteit- en schaalbaarheidsvoordelen van de cloud de business een stuk wendbaarder maakt.

Scenario 2: Beginnen met de migratie van Office 365, SharePoint en/of SaaS applicaties

Meteen helemaal de naar de cloud is voor veel bedrijven nog even te veel van het goede. Daarom willen de meeste organisaties eerst kleine stappen naar de cloud zetten. Dat doen ze door bijvoorbeeld met Office 365 te starten of enkele applicaties naar te Azure migreren. Dat gold ook voor een Nederlands bouwbedrijf. Ze wilden naar Office 365 en daarbij hun Active Directory Federation Services (ADFS) beveiligen. Ze waren namelijk bezorgd over de veiligheid van de Active Directory-gegevens. Om dat goed in te regelen, hebben ze de ADFS beveiligd met een WAF en de verbinding beveiligd met een NGF (figuur 2). Dit ging zo soepel dat de migratie niet in 9, maar in 3 maanden is gelukt.



Figuur 2

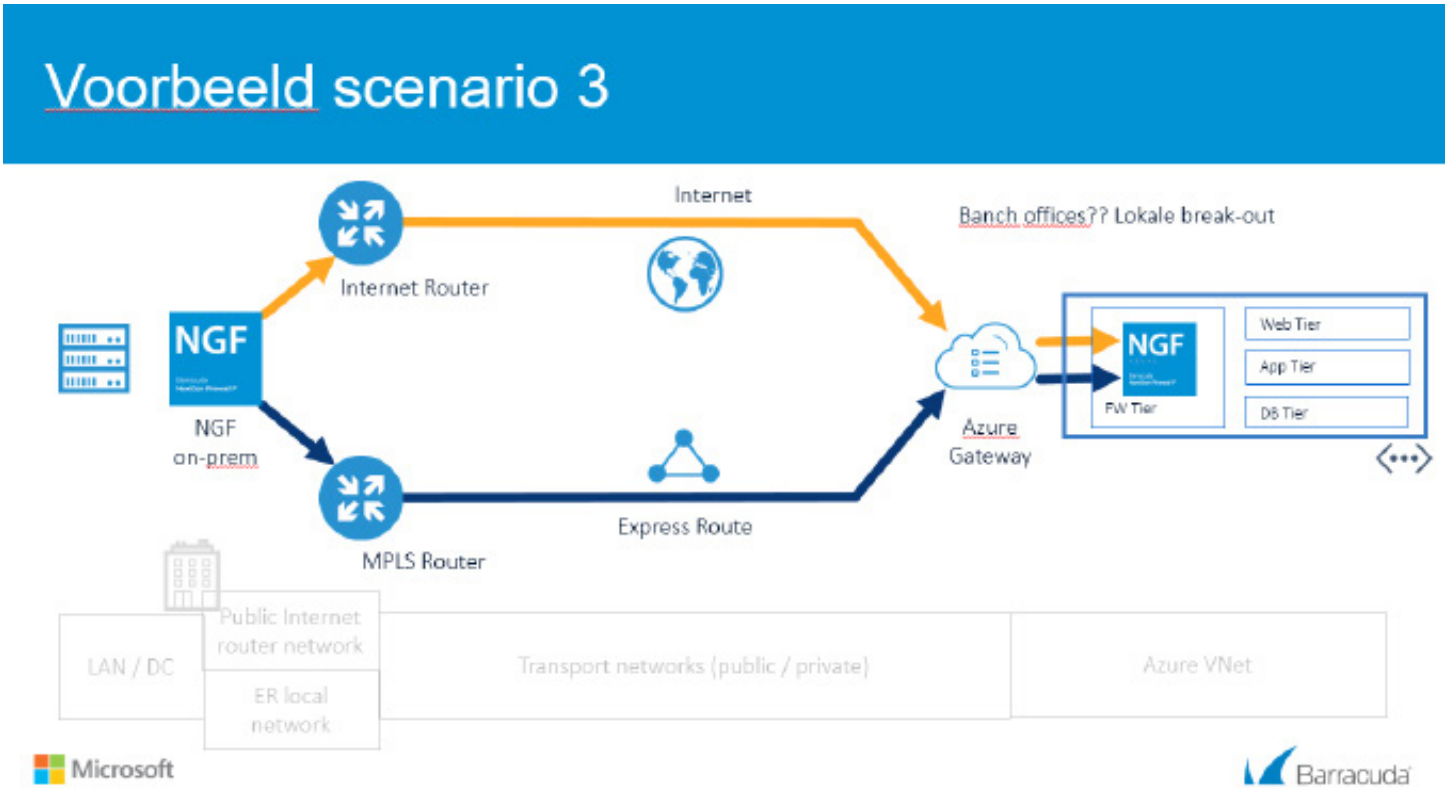
Scenario 3: Het migreren van virtuele machines naar de cloud met on-premise data

Een van de meest voorkomend use cases is een gedeeltelijke overstap naar de cloud waarin de data on-premise blijft staan; het hybride model. Dat is niet zo gek want in één keer een datacenter afschrijven is kostbaar. Langzaam uitfaseren en toch optimaal van de cloud profiteren is dan het adagium. Zorgverzekeraar Avitea migreert op deze manier ook op de langere termijn naar de cloud. Zo kunnen ze profiteren van de flexibiliteit en de schaalbaarheid zonder dat er direct grote investeringen te worden gedaan.

Het gevaar zou kunnen zijn dat er een kink in de kabel tussen de cloud en het on-premise datacenter ontstaat. Terwijl je juist door wil kunnen werken. Dankzij de support van Microsoft voor de lokale datacenters werd dat bereikt. Toen Avitea een ExpressRoute-probleem ondervond, werd dat automatisch opgelost door de rollover met het TINA-protocol (gele lijn in figuur 3) van Barracuda. Hierdoor werd een 100 procent uptime behaald.

Voor een zorgverzekeraar zijn de gegevens van klanten zeer privacygevoelig. Door het verkeer WAF en de NGF te beveiligen en te versleutelen, is de verbinding goed beveiligd. Door deze toepassingen heeft Avitea een geoptimaliseerde hybride verbinding.

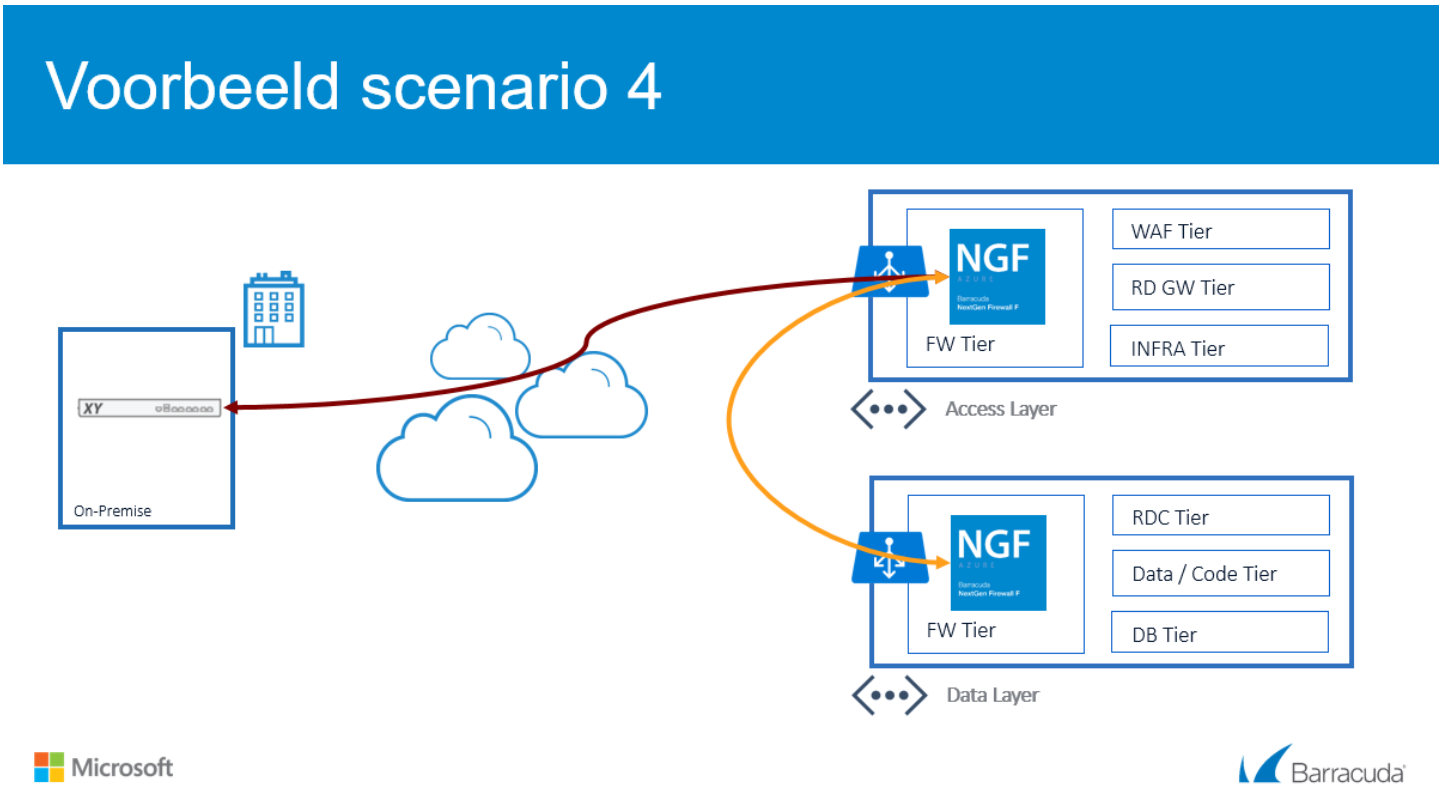
We zien dat er veel bedrijven verschillende gedistribueerde on-premise omgevingen hebben, nationaal of internationaal. Met een NGF kun je lokale break-out naar de public cloud realiseren. Daarmee hoef je geen duur global MPLS-contract aan schaffen. Met de NGF kun je prioriteit aan bepaalde verbindingen geven waarbij je tegelijk inzicht hebt in het dataverkeer. Welke data gaat via het gewone internetverkeer en welke gaat via de ExpressRoute en krijgt prioriteit?



Figuur 3

Scenario 4: het inrichten van de eigen private cloud

Kun je in de public cloud ook een eigen private cloud inrichten? Ja, dat kan. Zo wilde een ziektekostenverzekeraar Remote Desktop Services (RDS) voor externe gebruikers in de public cloud inrichten. Hierbij hadden ze zorgen over het uitgaande verkeer van het RDS-systeem. Daarnaast wilden ze de toegang natuurlijk gedegen beveiligen. Via een NGF wordt het verkeer gefilterd en met een WAF wordt de RDS veilig gepubliceerd. Ook in deze configuratie (figuur 4) wordt het verkeer volledig gemonitord.



Figuur 4

Wil je weten hoe je de migratie naar de cloud voor jouw organisatie het goed en veilig uitvoert?

2SOURCE4
Pure in business ICT
www.2source4.com

Barracuda

Microsoft