



Kies de juiste strategie voor cloudconnectiviteit

Profiteer als IT-manager van alle voordelen die de cloud te bieden heeft.
Vermijd de valkuilen van een ad-hoc aanpak.



Inhoud

01	Hoe dit whitepaper jou kan helpen	3
02	Uitdagingen voor IT-managers	4
03	Publiek internet versus directe laag-2-verbinding	5
04	Vier manieren om met de cloud te verbinden	7
05	Proof of Concept	10
06	Kies de beste oplossing voor jouw bedrijf	14
07	Praktische tips	15
08	Hoe wij jou hierbij ondersteunen	16
09	De volgende stap	17

Hoe dit whitepaper jou kan helpen

Te weinig bedrijven denken vooraf goed na over een passende strategie voor cloudconnectiviteit. Maak je vooraf niet de juiste keuzes, dan kan het juist een belemmerende factor worden voor het gebruik van de cloud en je bedrijfsvoering.

De cloud is niet meer weg te denken voor bedrijven. De voordelen zijn overduidelijk, bijvoorbeeld schaalbaarheid, flexibiliteit en kostenbesparingen. Bij het gebruik van de cloud komt ook connectiviteit kijken.

Vaak wordt pas goed nagedacht over de juiste strategie voor cloudconnectiviteit als het cloudgebruik toeneemt of als er issues ontstaan. Denk aan oplopende rekeningen, trage applicaties of gebrekkige support. Terwijl je dacht dat alles op orde was.

Kies daarom bewust voor de juiste oplossing. Er zijn talloze opties, vaak eenvoudiger en goedkoper dan je denkt. Je moet alleen weten welke factoren van belang zijn.

In deze whitepaper leer je alles over de cloud en cloudconnectiviteit. In hoofdstuk 2 bespreken we de uitdagingen waarmee je als IT-manager te maken kunt krijgen. Hoofdstuk 3 biedt een duidelijke uitleg over de verschillen tussen het publieke internet en een directe laag-2-verbinding.

Vervolgens behandelen we in hoofdstuk 4 de vier manieren om verbinding te maken met de cloud. In hoofdstuk 5 presenteren we de resultaten van een Proof of Concept, waarin we hebben onderzocht wat nu écht het verschil is tussen een directe laag-2-verbinding en een verbinding via het publieke internet.

Hoofdstuk 6 bevat een handig schema met alle belangrijke informatie per oplossing. In hoofdstuk 7 geven we zeven praktische tips om de juiste keuzes te maken op het gebied van cloudconnectiviteit voor jouw bedrijf, en tot slot vertellen we in hoofdstuk 8 hoe wij je hierbij kunnen ondersteunen.

Aan het eind weet je wat je moet doen om als IT-manager of IT-verantwoordelijke de controle te behouden met de juiste cloudconnectiviteitsstrategie. Zo vermijd je de valkuilen van een ad-hoc aanpak en profiteer je optimaal van alle voordelen die de cloud te bieden heeft.

Uitdagingen voor IT-managers

Zonder een doordachte strategie voor cloudconnectiviteit kun je vroeg of laat tegen flinke uitdagingen aanlopen. Denk aan sterk oplopende kosten, complex beheer en verlies van overzicht en controle.

Problemen ontstaan vaak op het verkeerde moment, zoals tijdens een grote migratie of bij toename van het aantal gebruikers. Hieronder beschrijven we enkele uitdagingen waarmee je als IT-manager te maken kunt krijgen:

Oplopende kosten

Bij het kiezen voor of het migreren naar een grotere clouddienst is het vaak moeilijk om de exacte kosten vooraf in te schatten. De kosten stijgen naarmate het gebruik toeneemt. Bovendien is bij een clouddienst zoals Microsoft Azure al het verkeer nāār de cloud gratis, maar betaal je voor al het uitgaande verkeer. Dat betekent: hoe meer data je uit de cloud haalt, hoe duurder. Gelukkig zijn daar slimme oplossingen voor.

Bijvoorbeeld: zet systemen die data uitwisselen bij elkaar, zodat die data binnen de cloud blijft. En haal daaruit alleen de data die je echt nodig hebt of neem een ongelimiteerd of vooraf betaald dataplan af om te weten waar je aan toe bent.

Complexiteit van het beheer

Het netwerklandschap wordt steeds complexer en minder tastbaar door de toename van verbindingen met verschillende cloudomgevingen. Elke cloudprovider hanteert eigen tools, methodes en interfaces, wat het beheer ingewikkelder maakt. Zeker als je gebruikmaakt van verschillende cloudomgevingen wordt het uitdagender om het netwerk overzichtelijk te houden.

Om deze complexiteit te managen, is het cruciaal dat je een doordachte cloudstrategie kiest. Zo'n strategie vraagt om gedegen onderzoek en documentatie. Het is raadzaam om hierbij de IT-partners te betrekken waarmee je samenwerkt.

Veiligheid en compliance

Het waarborgen van veiligheid en naleving van regelgeving is een cruciale uitdaging bij cloudconnectiviteit. Elke cloudprovider heeft zijn eigen beveiligingsmechanismen en standaarden. Waar staat je data? Hoe komt het daar? Is je data er veilig? Staat jouw data bij Amazon of Microsoft, dan wordt de metadata opgeslagen en beheerd in de Verenigde Staten.

Dat hoeft geen probleem te zijn, maar wees je bewust van mogelijke consequenties. Je wilt achteraf niet hoeven te melden dat je onvoldoende maatregelen hebt genomen. Met meerdere cloudomgevingen is het een uitdaging om de beveiliging goed te coördineren en gegevensoverdracht veilig te houden.

Prestatie en betrouwbaarheid

Als IT-manager moet je zorgen voor optimale prestaties en betrouwbaarheid van de connectiviteit. Dit kan uitdagend zijn, vooral bij meerdere cloudomgevingen. Factoren zoals latency, bandbreedte en netwerkcongestie spelen een rol. Strategieën, waaronder werken met meerdere internetproviders, directe verbindingen en continue monitoring van prestaties, kunnen hierbij helpen.



Wat is cloudconnectiviteit?

Cloudconnectiviteit verwijst naar de verbindingen tussen de IT-omgeving van jouw bedrijf of organisatie, externe gebruikers en de clouddiensten. Deze connecties kunnen op verschillende manieren worden gemaakt. Met de juiste strategie worden deze diensten integraal onderdeel van je IT-infrastructuur. Zo creëer je stabiele, veilige en snelle verbindingen.

Publiek internet versus directe laag-2-verbinding

Je kunt je clouddienst verbinden via het publieke internet of via een directe laag-2-verbinding. Voor een verbinding via internet kun je bijvoorbeeld gebruikmaken van SD-WAN of VPN. Maar het blijft publiek internet met zijn beperkingen, zelfs als je netwerk redundant is en je meerdere netwerkinfrastructuren toepast.

Een directe laag-2-verbinding loopt buiten het publieke internet om en is daardoor stabiel en veiliger. Lees hieronder meer over publiek internet versus een directe verbinding:

Publiek internet

Het internet bestaat uit een hiërarchie van netwerken, waaronder Internet serviceproviders (ISP's), bedrijfsnetwerken, datacenters van cloudproviders en andere netwerkproviders. Apparaten die verbonden zijn met het internet communiceren via gestandaardiseerde protocollen, zoals het Internet Protocol (IP) en het Border Gateway Protocol (BGP).

Elk apparaat op het internet is bereikbaar via een IP-adres, maar het weet niet de exacte route naar een ander apparaat of andere dienst. Daar zetten we ISP-routers voor in die gebruikmaken van BGP.

Border Gateway Protocol

Het routingsprotocol BGP speelt een essentiële rol in het functioneren van het internet. Het wordt gebruikt voor het uitwisselen van routinginformatie tussen autonome systemen (AS'en). Een AS is een netwerk of een groep netwerken onder

een gemeenschappelijke administratie en technische controle, zoals een ISP of een groot bedrijfsnetwerk.

Het BGP-protocol wordt vooral gebruikt om gegevenspakketten te routeren tussen verschillende AS'en. Het stelt routers in staat informatie uit te wisselen over beschikbare routes en de beste paden te selecteren voor het doorsturen van verkeer. Het BGP-protocol bepaalt continu de beste route voor verkeer vanaf jouw locatie naar bijvoorbeeld de cloud. Dit pad kan regelmatig veranderen door veranderingen bij andere ISP's op het internet.

Distributed Denial of Service (DDoS)-aanval

Een plotselinge verandering van BGP-routes kan worden veroorzaakt door een DDoS-aanval, die meestal plaatsvindt wanneer iedereen werkt. Het doel is immers om werkzaamheden te verstoren. Deze aanval hoeft niet eens gericht te zijn op jouw verbinding of clouddienst. Als ergens in de route een verbinding volloopt, kan dit zorgen voor wijzigingen aan de route. Dit kan de performance of betrouwbaarheid van je cloudconnectiviteit via het publieke internet beïnvloeden.

SD-WAN en publiek internet

Het toepassen van SD-WAN-technologieën om naar je cloud te verbinden kan zorgen voor een hogere betrouwbaarheid door meerdere ISP's per locatie te gebruiken. SD-WAN kiest continu de beste van de twee (of meer) verbindingen om de cloud te bereiken. Bij een DDoS-aanval bij provider 1, schakelt SD-WAN automatisch over naar de verbinding van provider 2. Echter, je maakt met SD-WAN nog steeds gebruik van het publieke internet en hebt geen controle over de gekozen route.

Directe laag-2-verbinding naar de cloud

De performance en betrouwbaarheid van cloudconnectiviteit via het publieke internet kunnen wisselen. Soms werkt een verbinding perfect, maar soms zijn er onverklaarbare vertragingen of uitval. Voor een IT-manager is niets zo vervelend als onvoorspelbaarheid. Vertragingen of verstoringen komen vaak voor op het moment dat het niet uitkomt. Daarom kiezen sommige bedrijven voor een directe laag-2-verbinding naar de cloud.

Cloud Exchange Providers

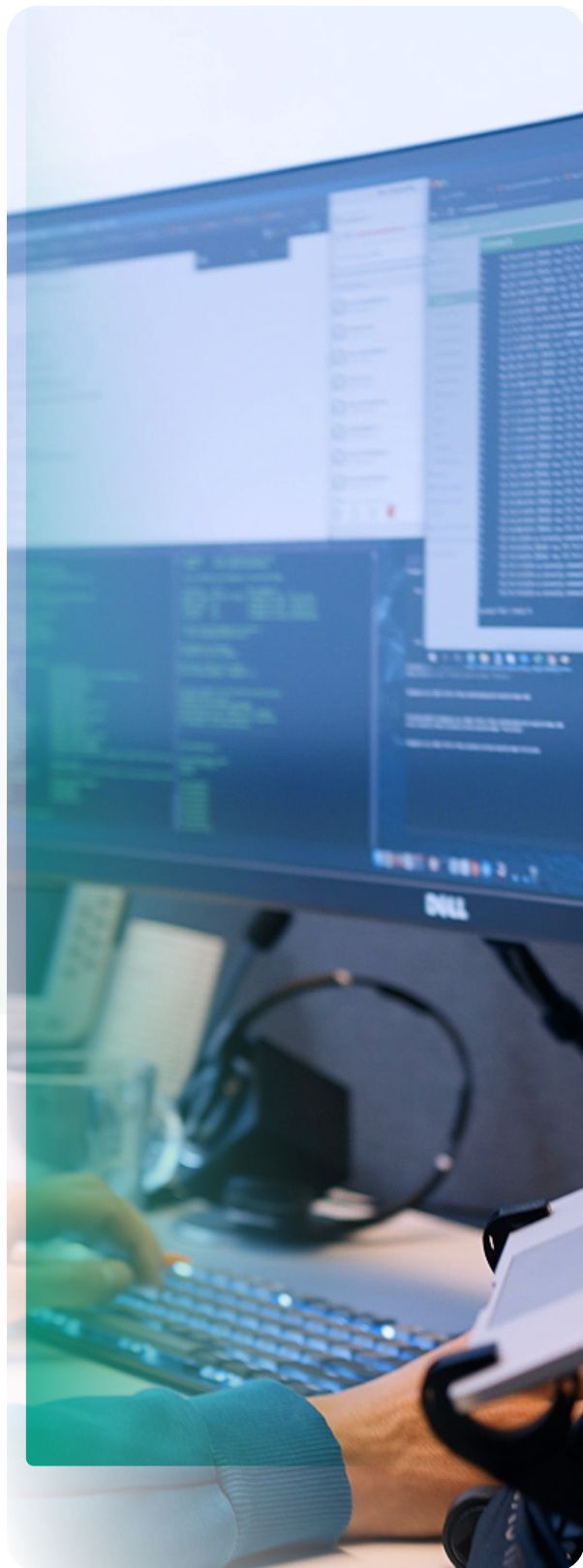
Grote, publieke cloudproviders kiezen voor snelle, directe verbindingen naar Cloud Exchange Providers. Verbindingen van soms wel meerdere malen 100 Gigabit per seconde. Deze Cloud Exchange Providers zijn vaak aanwezig in veel grote of eigen datacentra. Dit maakt het voor bedrijven makkelijker een directe koppeling te leggen met zo'n provider.

Als bedrijf heb je dan een directe koppeling met je cloudaanbieder(s) gemaakt, zonder dat je het publieke internet gebruikt of daarvan afhankelijk bent. Het is wel een koppeling naar één of meerdere datacentra van je Cloud Exchange Provider, maar deze koppeling is nog niet op je bedrijfslocatie aanwezig.

Managed Service Providers (MSP)

Een Managed Service Provider kan helpen om een directe verbinding te maken tussen jouw bedrijfslocatie(s) en de Cloud Exchange Provider(s). Via de verbindingen naar je bedrijfslocatie(s) kan de MSP een apart deel of zelfs volledig gescheiden verbinding leveren direct naar je cloudprovider.

Door de sterke groei van glasvezel, kan dit tegenwoordig tot wel 10 of 100 Gigabit per seconde. Bovendien kan een MSP al je bedrijfslocaties aansluiten op een Private Network. Dit vergemakkelijkt het onderlinge verkeer tussen je locaties en maakt het mogelijk de directe verbinding naar de cloudproviders direct aan te sluiten op al je locaties, in plaats van één-op-één-verbindingen van elke locatie naar de cloud.



Vier manieren om met de cloud te verbinden

Verbinding maken met cloudproviders zoals Microsoft Azure, Amazon AWS en Google Cloud kan op verschillende manieren. Wij helpen je graag een weloverwogen keuze te maken. In dit hoofdstuk beschrijven we vier veelvoorkomende methodes:

1. Openbaar toegankelijk vanaf het internet

In sommige situaties kan het slim zijn je clouddiensten direct vanaf het internet beschikbaar te maken, zonder VPN of directe verbindingen. Denk bijvoorbeeld aan deze situaties:

Openbare toegankelijkheid

Een goed voorbeeld zijn openbare cloudservices zonder gevoelige data, zoals een website of een API. Gebruikers kunnen de cloudservice bereiken via een openbaar IP-adres met een domeinnaam. Dit biedt de mogelijkheid om overal ter wereld gebruik te maken van de diensten.

Niet-gevoelige gegevens en lage beveiligingseisen

Als de cloudservice geen gevoelige gegevens bevat en lage beveiligingseisen heeft, kan rechtstreekse internetconnectiviteit zonder VPN of directe verbindingen volstaan. Bijvoorbeeld bij openbare informatiebronnen, onbelangrijke testomgevingen of demo-applicaties waarin nog geen data zit.

2. Cloudconnectiviteit via VPN

Een VPN-verbinding naar een cloudservice kan in verschillende situaties de voorkeur hebben. Vooral als er behoefte is aan extra beveiliging, privacy en controle. Denk bijvoorbeeld aan deze situaties:

Beveiligde gegevensoverdracht

Verwerkt de cloudservice gevoelige gegevens, zoals persoonsgegevens, bedrijfskritische informatie of vertrouwelijke klantgegevens? Dan is een VPN-verbinding met encryptie een goede oplossing om de gegevensbeveiliging te waarborgen. De versleutelde tunnel van een VPN beschermt de gegevensoverdracht bijvoorbeeld tegen afluisteren en inbraakpogingen.

Bescherming tegen externe bedreigingen

Een VPN-verbinding biedt extra bescherming tegen externe bedreigingen, zoals malware, phishing-aanvallen en onbeveiligde netwerken. Het versleutelen van de internetverbinding met een VPN voorkomt dat kwaadwillenden gegevens onderscheppen of manipuleren.

Compliance-eisen

Heeft jouw bedrijf te maken met specifieke compliance-eisen, bijvoorbeeld AVG (binnen Nederland), GDPR (in heel Europa) of HIPAA (Verenigde Staten)? Dan kan een VPN-verbinding nodig zijn om te voldoen aan de eisen voor gegevensbescherming en privacy.



Het rechtstreeks verbinden van een cloudservice met het internet is eenvoudig en goedkoop, maar zonder extra beveiligingslagen minder veilig en betrouwbaar.

Netwerksegmentatie en controle

Met een VPN-verbinding kan je netwerksegmentatie toepassen en specifieke toegangscontroles implementeren voor verschillende gebruikersgroepen of services. Dit biedt een extra beveiligingslaag waarmee je strikte controle hebt over wie toegang heeft tot welke delen van het netwerk en de cloudservice(s). Met netwerksegmentatie kun je bij een calamiteit uitsluitend focussen op de groep met toegang. Dat geeft rust en overzicht.



Deze methode kan extra configuratie vereisen en overhead met zich meebrengen. Het is belangrijk om de prestaties en schaalbaarheid van de VPN-oplossing te evalueren.

3. Cloudconnectiviteit via SD-WAN of SASE

Met SD-WAN (Software Defined Wide Area Network) en SASE (Secure Access Service Edge) beheer je je netwerken makkelijk en veilig. Beide technologieën verbinden al je locaties, datacenters en cloudverbindingen, ongeacht het type internetverbinding. Cloudconnectiviteit op basis van SD-WAN, in combinatie met virtuele SD-WAN-routers en geïntegreerde SASE-functionaliteiten in de cloud, biedt voordelen in verschillende situaties:

Geografisch verspreide locaties

Heeft jouw bedrijf meerdere geografisch verspreide locaties en wil je een uniforme en consistente connectiviteit naar de cloud? Dan zijn SD-WAN en SASE een goede keuze. SD-WAN creëert een geïntegreerd netwerk dat meerdere vestigingen en cloudservices verbindt, ongeacht hun locatie. Virtuele SD-WAN-routers in meerdere clouds zorgen ervoor dat je altijd verbonden bent. Het beheer is eenvoudig: via één centraal dashboard beheer je al je locaties en verbindingen.

Schaalbaarheid en flexibiliteit

SD-WAN in combinatie met virtuele SD-WAN-routers biedt schaalbaarheid en flexibiliteit bij het toevoegen of wijzigen van connectiviteitsopties. Je kunt snel nieuwe locaties aansluiten op het netwerk en de cloudconnectiviteit aanpassen aan veranderende behoeften. Dit vereist geen fysieke infrastructuur of handmatige handelingen.

Verbeterd inzicht en sturing op verkeersstromen

Een voordeel van SD-WAN is dat je niet alleen dynamisch kunt sturen op verkeersstromen, maar dat je er ook veel beter zicht op hebt. Je volledige netwerk is tot op detailniveau inzichtelijk en te beheren in één portaal.

Beveiliging en compliance

SD-WAN biedt geavanceerde beveiligingsfuncties om netwerkverkeer te beschermen, zoals versleuteling en geavanceerde firewalls. Met virtuele SD-WAN-routers in de cloud pas je eenvoudig consistente beveiligingsmaatregelen toe op alle locaties en cloudservices. Dit maakt het makkelijker om beveiligings- en privacyvoorschriften na te leven.

4. Cloudconnectiviteit via een directe laag-2-verbinding

Een directe laag-2-verbinding bevindt zich op de tweede laag van het OSI-model (Open Systems Interconnection); een referentiemodel voor de manier waarop toepassingen in een netwerk communiceren. De tweede laag richt zich op datalinkfuncties en zorgt voor betrouwbare en foutloze communicatie tussen twee apparaten op een lokaal netwerk (LAN).

Voor cloudconnectiviteit betekent dit dat de verbinding tussen het bedrijfsnetwerk en de cloudservice plaatsvindt op laag-2 (datalink-laag) van het OSI-model, zonder gebruik te maken van laag-3 (netwerk-laag) en IP-routing.

Een directe laag-2-verbinding naar cloudservices zoals Microsoft Azure, Amazon AWS of Google Cloud biedt voordelen in verschillende scenario's.

Wil je meer weten over SD-WAN? Op **deze pagina** vind je meer informatie inclusief onze podcast 'SD-WAN, nice to have of gamechanger?' met gastspreker Ben Radstaat van Cisco Meraki.

Hoge bandbreedte en lage latency

Een directe laag-2-verbinding is ideaal als je behoefte hebt aan hoge bandbreedte en lage latency tussen je lokale netwerk en de cloudservices. Dit is vooral belangrijk voor toepassingen met intensief dataverkeer, real-time interacties of grote gegevensoverdrachten.

Bij snelheden boven de 1 Gigabit per seconde biedt een directe laag-2-verbinding uitkomst. Deze verbindingen kunnen snelheden tot wel 100 Gigabit per seconde leveren en hebben vaak een veel lagere gegarandeerde latency dan verbindingen via het publieke internet.

Consistente prestaties

Met een directe laag-2-verbinding bereik je consistentere netwerkprestaties dan met verbindingen via het publieke internet. Dit is nuttig voor kritieke workloads die afhankelijk zijn van betrouwbare en voorspelbare netwerkprestaties. Een directe laag-2-verbinding heeft geen last van DDoS-aanvallen in het netwerk tussen jouw bedrijfsnetwerk en de cloud. Het heeft geen publiek IP-adres en koppelt het netwerk van jouw aanbieder direct aan dat van de cloudaanbieder.

Verbeterde beveiliging

Een directe laag-2-verbinding biedt extra beveiligingsvoordelen. Het is een dedicated en private verbinding tussen je netwerk en de cloudprovider. Je zet hiermee het openbare internet volledig buitenspel. Dat betekent: minder blootstelling aan externe bedreigingen vergeleken met het gebruik van openbaar internet.



Proof of concept

Om te testen wat écht het verschil is, hebben we de praktijk in uitvoering gebracht en voerden we een Proof of Concept (PoC) uit.

Er zijn verschillende opties voor cloudconnectiviteit. Maar wat betekenen deze vormen van connectiviteit? Welke impact hebben ze op een verbinding? En is een directe laag-2-verbinding altijd beter of sneller dan een verbinding over het publieke internet, of is er weinig merkbaar verschil?

Onze aanpak

Voor de PoC hebben we een Microsoft Azure-omgeving opgezet met drie typen verbindingen. Elke verbinding hebben we gekoppeld aan een zo goed mogelijk gescheiden omgeving. Daarbij kreeg elke verbinding een eigen resource group en deelden ze waar mogelijk geen resources. Alle verbindingen ontsloten we via het signetbreedband core-netwerk; ons netwerk met een eigen backbone.

De snelheid beperkten we tot 50 Mbps om onderlinge beïnvloeding te voorkomen. Per resourcegroep implementeerden we een identieke virtuele machine met dezelfde specificaties, regio en open poorten en hetzelfde besturingssysteem. Deze machines fungeerden als testdoelen voor elke verbinding naar Azure. Vervolgens testten we de kwaliteit van de diverse verbindingen met twee tests.

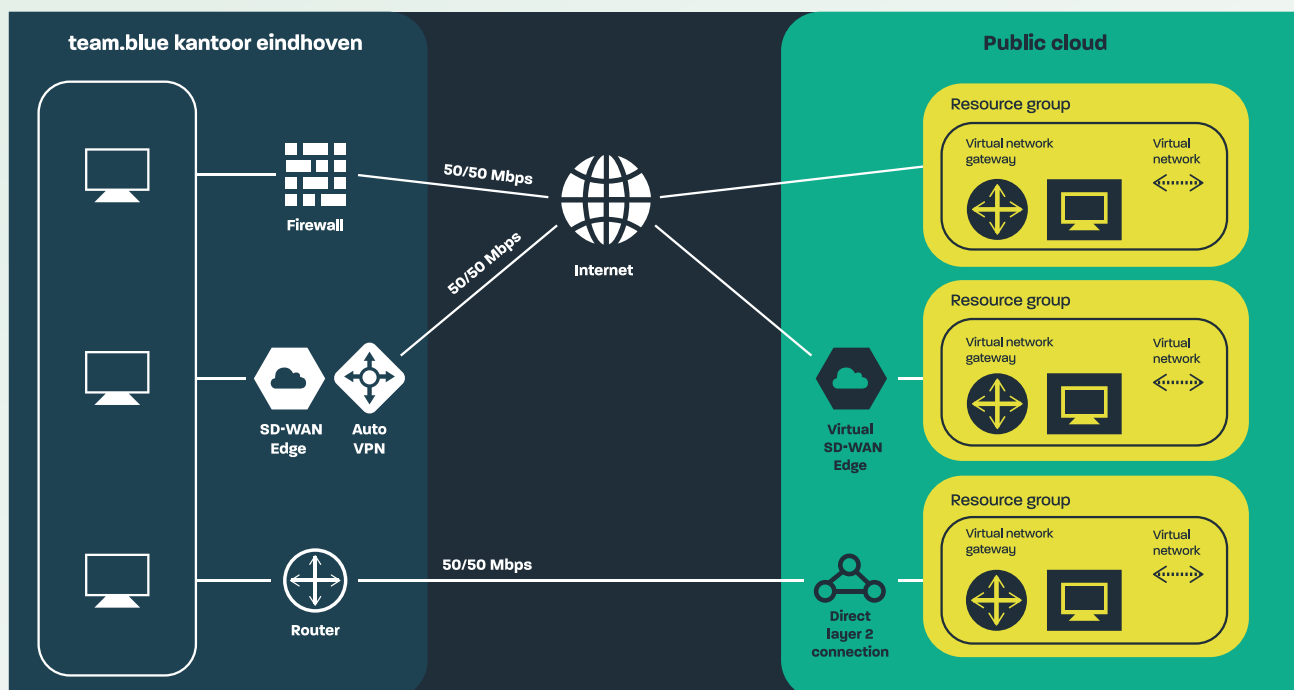
Test 1: Packetloss

Packetloss treedt op wanneer gegevenspakketten verloren gaan tijdens hun overdracht over een netwerk. Dit kan komen door congestie, netwerkstoringen, foutieve configuraties of problemen met netwerkapparatuur. Verloren pakketten moeten opnieuw worden verzonden, wat leidt tot vertragingen en verminderde doorvoer. Dit kan resulteren in onderbroken audio- of videostreams, trage verbindingen en verminderde prestaties van toepassingen die afhankelijk zijn van een betrouwbare en tijdige gegevensoverdracht. Kortom, packetloss kan grote gevolgen hebben voor de netwerkprestaties en de gebruikerservaring.

Test 2: Round-trip time (RTT)

RTT is een indicatie voor de vertraging in een netwerk, ook wel gezegd: de heen- en terugtijd. Deze hangt af van de fysieke afstand tussen apparaten, de netwerkarchitectuur, de kwaliteit van de netwerkverbinding en de belasting van het netwerk. Hoe lager de RTT, hoe sneller en responsiever de communicatie tussen apparaten. RTT wordt gemeten door een ping-verzoek (datapakket) te versturen vanaf een bronapparaat naar een bestemmingsapparaat, dat een ping-antwoord terugzendt.

Voor elke verbinding voerden we de pings uit met twee pakketgroottes: 56 bytes (het standaard ping-formaat) en 1000 bytes. Zo konden we de kwaliteit van een verbinding beter testen onder belasting en inzicht krijgen in hoe de verbinding omgaat met de opsplitsing van data (fragmentatie). En ook of er congestie (capaciteitstekort) optreedt bij hogere belasting van de verbinding.



Resultaten van de RTT-test

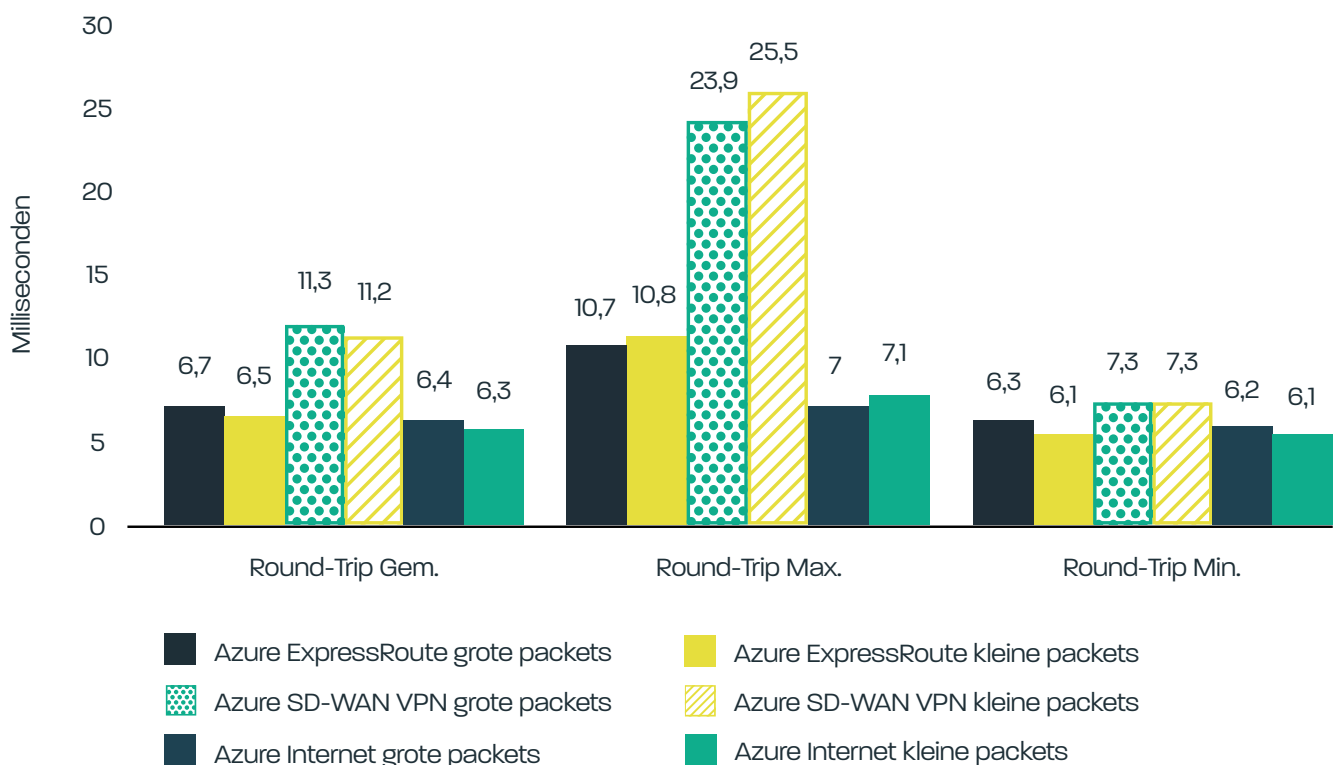
Uit de RTT-test bleek dat alle verbindingen over het algemeen goed presteren, zelfs in het slechtste geval bij een maximale RTT. Dit toont aan dat Nederland uitstekende internetverbindingen heeft, die vaak net zo snel zijn als een directe laag-2-verbinding.

Snelheden tot 30 milliseconden zijn meestal geen probleem, tenzij het gaat om videocommunicatie. Het is dus zeker niet zo dat alles boven 5 ms traag is. Wel kunnen de prestaties van verbindingen wereldwijd variëren.

In de tabel hiernaast zie je bij welke snelheden er impact is op de gebruikerservaring.

Een RTT van onder de 30ms is een voldoende snelle verbinding om op een normale manier correct over te werken. Dit laat ook onderstaande grafiek zien op basis van de verschillende packet-groottes van de Azure diensten.

RTT (ms)	Gebruikerservaring
<30	Geen of bijna geen impact op gebruikerservaring
30-60	Vrijwel geen impact, maar in sommige real-time communicatie merkbaar
60-100	De impact is merkbaar, maar over het algemeen is het nog goed werkbaar
100-150	Gebruikerservaring wordt hier ervaren als langzaam
>150	Er is verbinding, maar volgens huidige standaarden kan niet goed worden gewerkt



Alle maximale RTT-tests blijven onder de 30 ms, wat voldoende is voor betrouwbaar gebruik. Wel zagen we dat bij een hogere belasting van de internetlijnen, deze verbinding minder stabiel werd door het overige gebruik. Wanneer we kijken naar de gemiddelde en minimale resultaten van de tests geeft dit een goed beeld. Echter, de uitschieters (maximale) kunnen in sommige gevallen problemen geven.

Opvallend is dat zowel de ExpressRoute-verbinding (de directe laag-2-verbinding) als de directe internetverbinding (zonder beveiliging of versleuteling) de snelste RTT laten zien. De SD-WAN-verbinding ervaart iets hogere RTT-waarden door de toevoeging van VPN. Aan de andere kant heeft signetbreedband peerings met Microsoft voor de directe internetverbinding. Dit betekent dat het soms sneller kan zijn een pad te nemen via het directe internet dan via de ExpressRoute. Bij normaal verkeer, zonder DDoS-aanvallen of andere problemen, kan een directe internetverbinding dus sneller zijn. De ExpressRoute is echter de veiligste optie bij problemen op het internet.

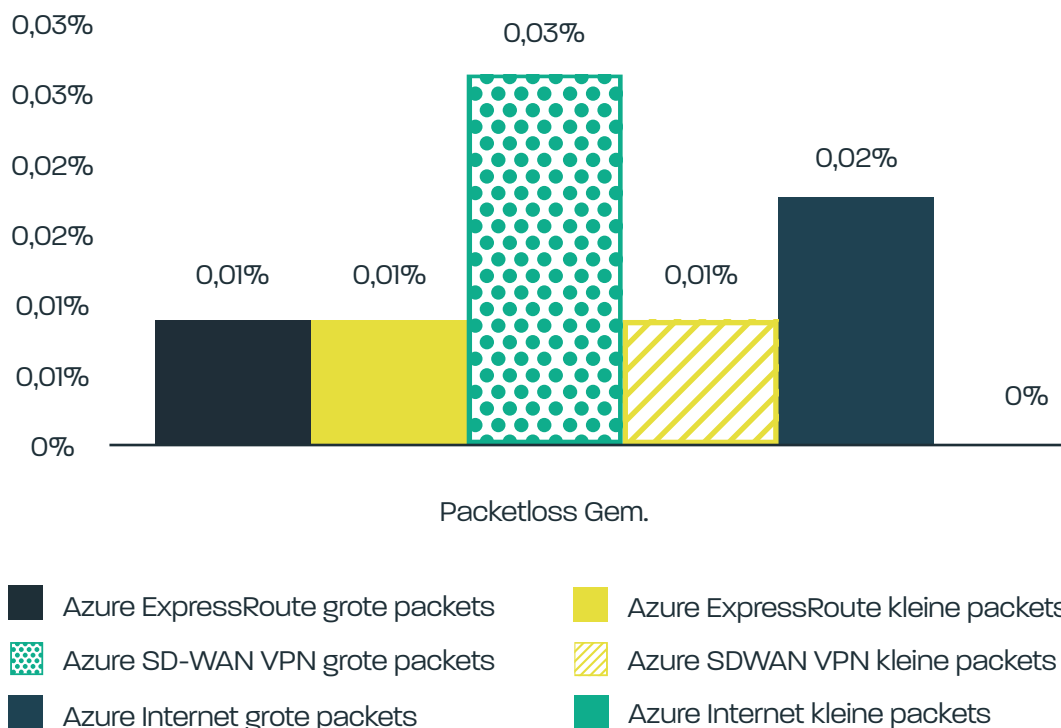
Resultaten van de packetloss-test

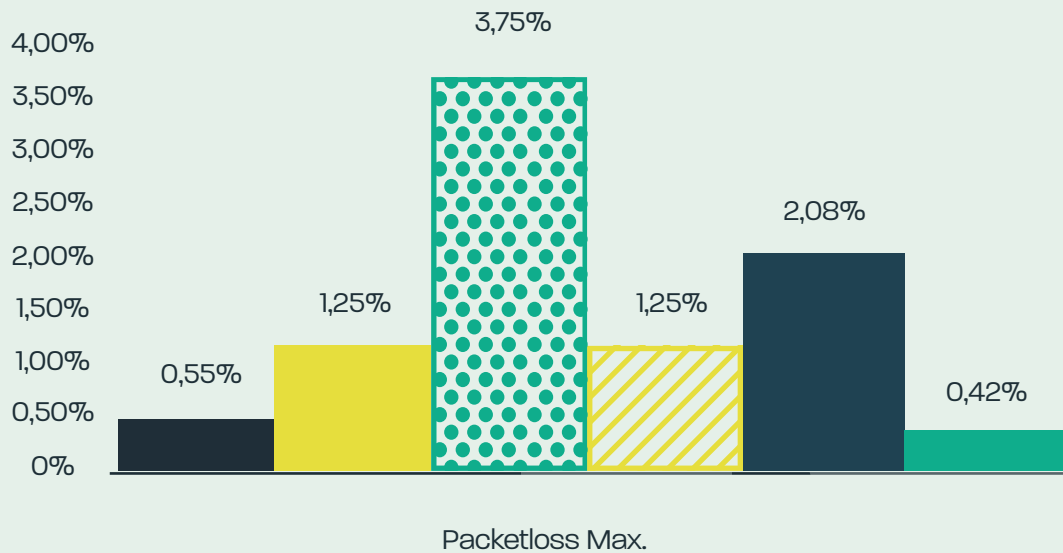
Bij de RTT-test bleken alle verbindingen voldoende snelheid te hebben. Maar bij de packetloss-test bleek dat niet altijd het geval. Een betrouwbare verbinding heeft meestal een zeer laag packetloss-

percentage, vaak onder de 0,1%. Het TCP-protocol verzendt niet-aangekomen pakketten opnieuw, zodat gebruikers hier geen hinder van ondervinden.

Sommige verbindingen hadden een packetloss van 3% tot 5%, voor normaal internetgebruik nog acceptabel, zolang voldoende bandbreedte beschikbaar is. Het TCP-protocol compenseert dit door pakketten opnieuw te verzenden. Bij video- en audiocommunicatie, die vaak het UDP-protocol gebruiken, wordt het pakket echter niet opnieuw verzonden. Dit betekent dat zelfs een klein percentage packetloss al verstoringen kan veroorzaken. Een packetloss van meer dan 2% resulteert vaak in wegvallende verbindingen of beeldblokken tijdens een video call. Dit benadrukt het belang van een betrouwbare verbinding met een laag packetloss-percentage, vooral voor real-time video- en audiocommunicatie.

Als we kijken naar de gemiddelden van alle geteste verbindingen, dan zien we dat alle verbindingen het gemiddeld heel goed doen, met waarden onder de 0,03%.





- | | |
|--|---|
|  Azure ExpressRoute grote packets |  Azure ExpressRoute kleine packets |
|  Azure SD-WAN VPN grote packets |  Azure SD-WAN VPN kleine packets |
|  Azure Internet grote packets |  Azure Internet kleine packets |

Uitschieters

Bij de maximale gemeten packetloss komt de directe internetverbinding en SD-WAN VPN met grote pakketgroottes boven de 2% uit. De ExpressRoute blijft in alle gevallen onder de 2% packetloss. Opvallend is dat de directe laag-2-verbinding beter omgaat met de segmentatie van grotere pakketgroottes, terwijl verbindingen via het internet hier meer hinder van ondervinden.

Kies de beste oplossing voor jouw bedrijf

Er bestaat niet zoiets als een one-size-fits-all benadering. Voor elke toepassing is er een beste keuze, maar die is niet voor alle toepassingen hetzelfde.

Geen enkele verbinding is in alle gevallen de beste keuze. Verschillende verbindingen hebben hun eigen voordelen en nadelen, afhankelijk van de

specifieke vereisten en behoeften van het bedrijf. signetbreedband helpt je hierbij.

Hoe we dat doen lees je in de hoofdstukken hierna. Om je alvast op weg te helpen met het kiezen van de juiste oplossing voor jouw bedrijf, vind je hieronder in een handig overzicht belangrijke informatie rond de voorwaarden en de voor- en nadelen per oplossing.

Verbindings - methode	Gebruikers-toepassing	Voordelen	Nadelen
Publiek internet	• Websites en openbare API's • Test en ontwikkeling	• Wereldwijd toegankelijk • Gemakkelijk schalen • Geen speciale hardware nodig	• Lage beveiliging • Mogelijk een hogere latency • Afhankelijk van publiek internet
VPN	• Beveiligde toegang tot interne applicaties of bedrijfsdata	• Extra beveiliging • Relatief eenvoudig op te zetten	• Mogelijke een hogere latency door encryptie • Beperkte maximale bandbreedte • Mogelijk complex
SD-WAN	• Zelfde als VPN • Meerdere locaties • Flexibele netwerk-beheeropties	• Eenvoudig centraal beheer • Flexibel en schaalbaar • Goede beveiliging en prestaties	• Vereist specifieke apparatuur • Kosten voor beheer en monitoring
Directe laag-2-verbinding	• Toepassingen met intensief dataverkeer • Noodzaak voor hoge beveiliging • Lage latency vereisten	• Gegarandeerd lage latency • Hoge mogelijke bandbreedte • Betrouwbaar en stabiel • Extra beveiliging	• Mogelijk hogere kosten • Complexere installatie en beheer

Praktische tips

Waar doe je verstandig aan? Hier zijn zeven praktische tips voor de juiste cloudconnectiviteitsoplossing.

Het aantal bedrijven dat gebruikmaakt van clouddiensten is tussen 2013 en 2023 meer dan verdubbeld. In Nederland gaat het inmiddels om 61% van alle bedrijven, meer dan het Europese gemiddelde. Tegelijkertijd verandert het cloudlandschap voortdurend en waarschijnlijk ook de behoeften van je bedrijf.

1. Zorg dat je vooraf de eisen goed in beeld hebt

Breng de eisen van elke cloudapplicatie of -dienst helder in kaart. Welke wettelijke vereisten gelden voor dataversleuteling? Vanaf welke locaties moeten gebruikers toegang hebben? Hoe redundant is de aanbieder en wat zijn de vereisten van je bedrijf? Alleen met een volledig overzicht kun je de juiste cloudconnectiviteitskeuze maken.

2. Kijk verder dan morgen

Clouddiensten evolueren snel door technologische ontwikkelingen zoals 'Infrastructure as Code' en Kubernetes. Bedrijven veranderen ook. Zijn je verbindingen flexibel genoeg om te migreren naar een andere (publieke) cloud als dat nodig is? Zorg dat je infrastructuur future proof is.

3. Zorg voor goede actuele documentatie

Beschrijf je cloudlandschap grondig en houd de documentatie actueel. Goede documentatie is cruciaal voor kennisoverdracht en verantwoordelijkheidsoverdracht. Elke applicatie komt tegenwoordig met zijn eigen as-a-servicedienst en draait op een andere locatie in de cloud. Zorg dat je altijd weet waar welke data staat en hoe je cloudinfrastructuur in elkaar steekt om grip te houden op je cloudlandschap.

4. Maak een risicoanalyse

Analyseer de kosten en gevolgen van een tijdelijke onbereikbaarheid van clouddiensten, inclusief omzetverlies, reputatieschade, boetes en impact op medewerkers, leveranciers en klanten. Kijk ook naar de omgeving: het gebied waarin je pand staat. Wordt er veel verbouwd of worden wegen aangelegd? Dan is er een groter risico op onderbreking van de cloudconnectiviteit.

Bepaal de impact op de bedrijfsvoering wanneer je geen verbinding meer hebt vanuit je bedrijfslocatie(s) naar de cloud. Kunnen medewerkers thuis verder werken of valt het productieproces stil?

5. Neem Business Managers mee in het proces en beslissingen

Betrek het management bij beslissingen over cloudconnectiviteit. Vraag naar de belangrijkste processen die altijd moeten blijven draaien, de maximale downtime en de cruciale IT-onderdelen. Maak een kostenberekening van mogelijke downtime en verzamel eisen en wensen van business managers voor hun afdelingen.

6. Kies de beste cloud voor elke toepassing

Voor nieuwe SaaS- of clouddiensten wil je per applicatie de beste locatie kiezen. Je cloudconnectiviteit moet dit mogelijk maken zonder beperkingen. Flexibiliteit is cruciaal om te kunnen wisselen tussen verschillende publieke clouds, afhankelijk van hun aanbod en prijsmodellen. Misschien is Google Cloud momenteel het beste platform voor het beheren van clusters van containerapplicaties en services, maar dit kan over enkele maanden heel anders zijn.

7. In gesprek met de leveranciers

Bespreek je eisen en wensen met je leveranciers. Directe laag-2-verbindingen naar grote clouds (zoals Microsoft Azure, Amazon AWS en Google Cloud) zijn gebruikelijk en hoeven niet duur te zijn. Als een directe verbinding niet nodig of te kostbaar is, kan een SD-WAN-oplossing een goede oplossing zijn om locaties redundant te verbinden met publieke clouds.

Van analyse en evaluatie naar oplossing

Wil je concreet werk maken van cloudconnectiviteit? Analyseer dan eerst de behoeften van je bedrijf. Wat is de bestaande situatie? Kan het beter? Wat heb je écht nodig; nu en in de toekomst? Evalueer de mogelijkheden van verschillende cloudproviders en kies de juiste oplossing. Het is goed om de clouddiensten echt te omarmen, zodat je er optimaal gebruik van maakt en de diensten voor je gaan werken.

Dit hoeft niet te betekenen dat je alles onderbrengt bij één cloudprovider. Kies de juiste plek voor het juiste doel. Het kan erop neerkomen dat je meerdere cloudproviders betreft, hybride cloudarchitectuur implementeert of gebruikmaakt van cloudagnostische netwerkoplossingen.

Een holistische benadering van connectiviteit en samenwerking met andere belanghebbenden binnen het bedrijf kunnen helpen om de juiste strategie voor cloudconnectiviteit te definiëren en te implementeren. En dat is precies de aanpak van signetbreedband!

Hoe wij jou hierbij ondersteunen

Bij signetbreedband begrijpen we dat cloudconnectiviteit een uitdaging kan zijn. Daarom bieden wij volledige ondersteuning, van initiële keus tot de inrichting.

Inventarisatie

Onze ondersteuning begint met een gedetailleerd gesprek om jouw eisen en gewenste cloudstrategie in kaart te brengen. We voeren een gedegen analyse uit van de huidige infrastructuur en connectiviteit en het huidige cloudgebruik. Hoe beter we het bedrijf en de groeiambities begrijpen, des te gericht kunnen we in een vroeg stadium meedenken over de meest geschikte connectiviteitsopties en -strategieën voor jouw specifieke situatie.

Advies uitbrengen

Op basis daarvan brengen we een advies uit. Daarbij helpen we je de juiste keuze te maken tussen de diverse vormen van cloudconnectiviteit en de integratie met je huidige netwerk.

High-level design

Vervolgens creëren we een high-level design. Samen bepalen we de beste inrichting van je cloudconnectiviteitsoplossing. Voor elke applicatie en elk doel bepalen we samen de optimale locatie. Onze visie is dat connectiviteit geen beperkende factor mag zijn voor de keuze van de juiste cloudoplossing. Dit kan bijvoorbeeld door te kiezen voor SD-WAN of een private netwerkoplossing. Door vooraf de juiste keuzes te maken, verminderen we het risico op belemmeringen bij een latere overstap naar een andere cloud.

Implementatie

signetbreedband fungeert graag als de hub tussen je locaties en (cloud)applicaties. Wij zorgen voor een naadloze implementatie van de gekozen cloudconnectiviteitsoplossing en integreren deze met je bestaande infrastructuur en cloudproviders. Proactieve ondersteuning zorgt voor een soepele overgang tijdens de implementatie.

Monitoring en beheer

Wij kunnen het beheer van de connectiviteit volledig op ons nemen, zodat prestatie- of beveiligingsproblemen 24/7 worden gedetecteerd en opgelost. Periodiek overleggen we over eventuele aanpassingen of optimalisaties die nodig zijn naarmate de behoeften van jouw bedrijf veranderen.

Onze aanpak garandeert een naadloze connectiviteit met de cloud, zodat je maximaal profiteert van de schaalbaarheid, flexibiliteit en kostenbesparingen die de cloud te bieden heeft.

IP Private Network als oplossing voor complexe directe laag-2-verbinding

Met een directe laag-2-verbinding verbind je de cloudomgeving rechtstreeks aan één van je locaties. Dit biedt de meeste zekerheid, stabiliteit en veiligheid. Maar wil je de cloudinfrastructuur uitbreiden met extra locaties of cloudproviders? Dan kan het al snel complex en kostbaar worden naarmate je meer locaties en cloudverbindingen toevoegt. Je moet namelijk voor elke nieuwe locatie en cloud een nieuwe directe laag-2-verbinding aanleggen.

Een IP Private Network (IPPN) van signetbreedband lost deze uitdaging op. Wij sluiten al je locaties aan op ons eigen core-netwerk, waardoor ze onderling verbonden zijn in één groot privénetwerk voor je complete IT-omgeving. De directe laag-2-verbinding van elke cloudomgeving wordt op dit netwerk aangesloten. Zo zijn huidige én toekomstige locaties automatisch verbonden met alle cloudverbindingen. Per cloudomgeving heb je slechts één enkele of redundante directe laag-2-verbinding nodig. De complexiteit van losse verbindingen wordt hiermee meteen opgelost.

Het beheren van meerdere losstaande directe laag-2-verbindingen zorgt niet alleen voor een verlies aan overzicht. Het geeft ook aanzienlijke configuratie-uitdagingen in je cloudomgevingen. Hiervoor zijn vaak geavanceerde routingstechnieken zoals BGP vereist, specialistische kennis die IT-managers of systeembeheerders mogelijk niet hebben. Bij een IPPN van signetbreedband regelen ons core-netwerk en onze netwerkexperts de volledige routing voor al je locaties en cloudomgevingen.

Ook het toevoegen van een nieuw (virtueel) netwerk of subnet aan je cloudomgeving hoeft geen probleem te zijn. Dit wordt door dynamische routingsprotocollen automatisch beschikbaar voor alle locaties binnen het IPPN. Breid je je infrastructuur uit met een nieuwe locatie? Ook die locatie krijgt direct toegang tot al je cloudomgevingen en andere locaties.

Zo profiteer je van de voordelen van een directe laag-2-verbinding zonder de nadelen van een hoge complexiteit en onnodig hoge kosten.



Binnen team.blue werken we nauw samen met clouddiensten van partners zoals TransIP en Proserve. Onder één dak ontwikkelen we multi-cloudoplossingen, gehost in Nederland.



09

De volgende stap

In deze whitepaper heb je concrete handvatten gekregen voor het ontwikkelen van een doordachte strategie voor cloudconnectiviteit. Klaar voor de volgende stap?

Neem contact op met onze specialisten. Gebruik de dikgedrukte link in het kader hieronder om vrijblijvend een gesprek in te plannen of gebruik de contactgegevens op de volgende pagina.

Samen zorgen we ervoor dat de verbinding naar de cloud optimaal wordt ingericht, zodat jouw bedrijf niet wordt beperkt, maar juist maximaal profiteert van de mogelijkheden die de cloud te bieden heeft.

Plan hier vrijblijvend een gesprek in

Wil je meer praktische voorbeelden? **Bezoek onze website** voor use cases van zowel SD-WAN als IPPN.

Over signetbreedband:

- ✓ **Een onafhankelijke netwerk solutions partner:** Specialist in connectiviteit en infrastructuurontwerp, gericht op continuïteit en hoge beschikbaarheid.
- ✓ **Heeft ervaring en expertise:** Meer dan 25 jaar ervaring en een uitgebreid partnernetwerk.
- ✓ **Heeft een eigen core-netwerk:** Biedt alle benodigde functionaliteit en capaciteit.
- ✓ **Onderdeel van team.blue:** Onderdeel van toonaangevend Europees tech powerhouse, met toegang tot een breed scala aan experts en middelen.
- ✓ **Gecertificeerd:** ISO 27001, ISO 9001, en NEN 7510, wat staat voor de hoogste normen in informatiebeveiliging en kwaliteitsmanagement.

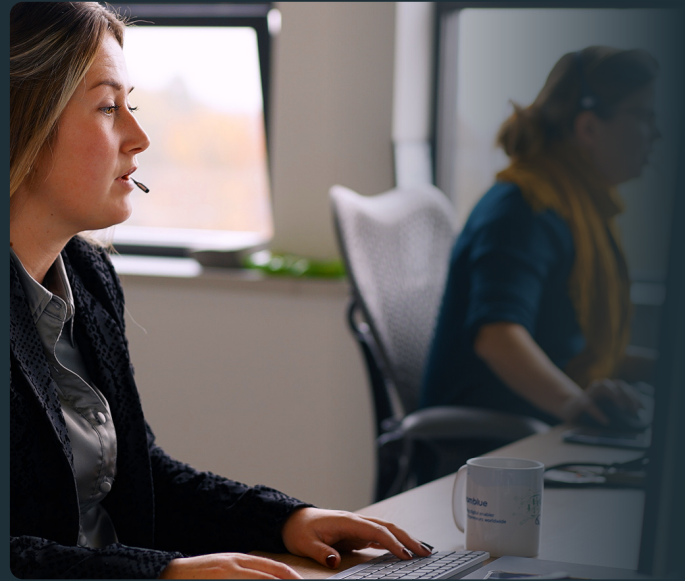


signetbreedband is een onafhankelijke netwerk solutions provider. We zijn er voor iedereen die op zoek is naar goede connectiviteit. We vereenvoudigen processen en ontwerpen infrastructuren die perfect passen bij jouw bedrijfsbehoeften.

Door te werken met modulaire bouwstenen maken we netwerken eenvoudig te beheren, wat resulteert in continuïteit en hoge beschikbaarheid. Onze klanten variëren van mkb'ers tot grotere bedrijven met meerdere locaties, zowel binnen als buiten Nederland. Met meer dan 25 jaar ervaring en een uitgebreid netwerk van partners, bieden wij alle functionaliteit en capaciteit die je nodig hebt via ons eigen core-netwerk.

Onderdeel van team.blue

signetbreedband opereert met een team van 55 experts in Arnhem en Eindhoven en is onderdeel van team.blue, een toonaangevende Europese aanbieder van webhosting en cloudcomputing. Dankzij deze samenwerking hebben we toegang tot een breed netwerk van specialisten en middelen, waardoor we optimaal kunnen inspelen op marktvraag.

**We helpen je graag**www.signetbreedband.nl

088 - 599 99 99

info@signetbreedband.nl