

Dienstbeschrijving

IP VPN

RoutIT

Datum: 2015

Versielog RoutIT

IP-VPN	06-05-2015
IP-VPN (Standaard)	17-05-2016
IP-VPN Plus (Open)	04-05-2015
IP-VPN (Plus) Beheer	21-10-2015
IP-VPN Voice	17-08-2015
IP-VPN Parent-Child	04-05-2015
BGP	04-05-2015
Verantwoordelijkheden, CPE en SLA	04-05-2015

Inhoudsopgave

1	IP VPN.....	4
2	IP-VPN (standaard)	5
3	IP-VPN Plus (open)	5
4	IP-VPN (Plus) Beheer (info t.b.v. CBG Connect)	6
5	IP-VPN Voice.....	8
6	IP-VPN Parent-Child.....	8
7	BGP.....	9
8	Verantwoordelijkheden CPE en SLA	10
9	Algemene kaderzetting van deze dienstbeschrijving	11

1 IP VPN

Door het inzetten van MPLS binnen het RoutIT netwerk, is het netwerk optimaal te gebruiken voor gecombineerde diensten zoals data, voice en video.

Binnen het RoutIT MPLS-netwerk is het hierdoor mogelijk MPLS IP-VPN's te creëren. Deze IP-VPN's zijn technisch gezien gescheiden routingstabellen op de routers binnen het RoutIT netwerk. Voor iedere klant wordt een apart label (uniek kenmerk) aan een IP-pakket toegevoegd. Zo is het mogelijk om op basis van het label en bijbehorende route unieke beslissingen te maken en voor iedere IP-VPN een "eigen" routingstabel aan te leggen. Ook zorgt dit aparte label ervoor dat elke IP-VPN security technisch gescheiden is van een andere IP-VPN.

Met RoutIT IP-VPN kunt u eenvoudig en op veilige wijze één of meerdere bedrijfsnetwerken, bedrijfslocaties en thuiswerkers verbinden tot een privénetwerk. Hiermee bent u in staat om het MKB een passende oplossing te bieden, waarbij hoge investeringen voor de eindgebruiker uitblijven.

IP-VPN varianten

RoutIT biedt verschillende IP-VPN varianten, afgestemd op de toepassing en behoeften van uw klant:

- IP-VPN
- IP-VPN Plus
- IP-VPN Plus Open
- IP-VPN Voice
- IP-VPN Beheer (Plus)

Daarnaast is het mogelijk om gebruik te maken van de IP-VPN Parent-Child constructie voor diverse IP-VPN varianten.

Overzicht

	IP-VPN	IP-VPN Plus	IP-VPN(Plus) open
Diensten	Alle	Alle	Alle
IP adressen	Private (rfc1918)	Private (rfc1918)	Publiek
Max IP adressen¹	256	-	-
Connectivity	Alleen PPP	PPP + routing	PPP + routing
Redundancy	Geen	BGP	BGP
mShield	V	V	X
mSSL	V	V	X
mVPN thuiswerk	V	V	X

RoutIT IP-VPN heeft de volgende kenmerken:

- Eén transparant geïntegreerd netwerk
- Maximaal 300 routes in één IP-VPN (ongeveer 130 verbindingen), met uitzondering van IP-VPN Voice
- Keuze uit meerdere leveranciers (Tele2, KPN, Eurofiber, NDIX)
- Een ruim assortiment van verbindingen
- Centraal beveiligde internettoegang vanuit de RoutIT-backbone
- Redundant en loadbalanced verbindingen²
- Verkeer dynamisch routeren³
- Back-up verbinding (bijv. DSL of BGP)
- Thuiswerkers te koppelen door mSSL en/of mVPN thuiswerker groep
- Layer 2 Class of Service mogelijk
- Eenvoudige integratie van Colocatie diensten
- Eenvoudig beheer door IP-VPN (plus) Beheer

2 IP-VPN (standaard)

Wat is een IP-VPN?

Conceptueel is een IP-VPN een virtuele router voor alle netwerk diensten. Alle door RoutIT geleverde diensten zijn aan te sluiten op deze virtuele router.

Een RoutIT IP-VPN is volledig afgescheiden van het internet. Dit houdt in dat de dienst geheel gesloten wordt aangeboden. Met mShield (firewall) ontsluit u alle vestigingen binnen een IP-VPN naar het internet. Deze firewall wordt centraal beheerd door de CSP voor alle vestigingen binnen de IP-VPN en zorgt voor een maximale performance. mShield is optioneel te bestellen bij de standaard IP-VPN.

Technisch

De klantlocaties worden binnen een IP-VPN permanent met elkaar verbonden door middel van de RoutIT MPLS backbone. Deze dienst maakt dus geen gebruik van het internet als transportmedium. De beveiliging van data is verzekerd, omdat het dataverkeer het RoutIT netwerk niet verlaat. Hierdoor is het mogelijk om end-to-end garanties af te geven. Dit geldt zowel voor de beschikbaarheid van de IP-VPN als voor de netwerkprestaties.

Binnen deze IP-VPN is het mogelijk om diensten op een standaard manier te koppelen. Hierbij wordt gebruikt gemaakt van PPP (gebruikersnaam en wachtwoord) en van oplossingen op de CPE (klantlocatie). Er is geen dynamische communicatie mogelijk tussen het klantnetwerk en het RoutIT IP-VPN.

Binnen de IP-VPN wordt er standaard gebruik gemaakt van private IP adressering* (RFC1918). Het is mogelijk tot 256 IP adressen** (/24) op 1 verbinding te plaatsen.

* *Publiek adressering is mogelijk binnen een IP-VPN, maar moet worden overlegd met RoutIT.*

** *Meer dan 256 IP adressen kunnen worden toegekend indien u gebruikmaakt van een IP VPN Plus i.c.m. BGP.*

Redundancy

Redundancy is in deze IP-VPN alleen mogelijk door een stand-by lijn te gebruiken, welke niet actief is (geen PPP sessie actief) en deze pas te activeren als de primaire verbinding niet meer werkt. Deze oplossing kan alleen ingesteld worden op de CPE (klantrouter) en wordt niet actief ondersteund door RoutIT.

RoutIT staat toe dat voor de stand-by lijn een Thuiswerker-verbinding wordt gebruikt, die op het moment van een failover of backup-situatie wel het subnet van de primaire verbinding routeert als de andere lijn een verbinding van het type Zakelijk is.

3 IP-VPN Plus (open)

Kenmerken IP-VPN Plus

IP-VPN Plus bevat alle eigenschappen van een IP-VPN, met als aanvulling de mogelijkheid om een routeringsprotocol te activeren. Hierdoor is het mogelijk om meerdere subnets op 1 locatie te plaatsen en is het mogelijk redundancy toe te passen.

Het enige routerings protocol dat door RoutIT wordt ondersteund is BGP.

De IP-VPN Plus is geschikt voor private en eventueel publieke IP's*.

* *Publiek adressering is mogelijk binnen een IP-VPN, maar moet worden overlegd met RoutIT.*

Kenmerken IP-VPN Plus Open

IP-VPN Plus Open bevat alle redundancy-eigenschappen van een IP-VPN Plus, maar is alleen geschikt voor publieke IP's. IP-VPN Plus Open is direct gekoppeld aan het publieke internet (zonder mShield).

Technisch

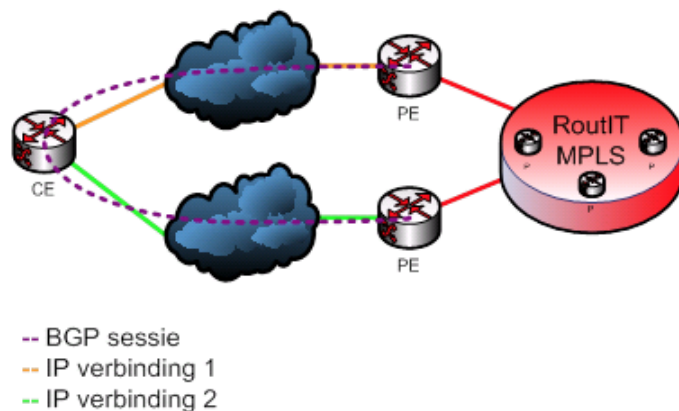
Het routeringsprotocol Border Gateway Protocol (BGP) wordt ondersteund, en biedt mogelijkheid meerdere subnets te transporteren of redundancy toe te passen.

Met BGP is het mogelijk om routes uit te wisselen en tevens extra attributen per route mee te geven. Hierdoor is het mogelijk om voorrang aan bepaalde routes te geven waardoor de CPE op klantlocatie kan bepalen wat er met de routes moet gebeuren (zowel inkomend als uitgaand). Iedere BGP sessie bestaat uit één of meerdere TCP sessies, waardoor het mogelijk is om storingen in de onderliggende domeinen (klant, telco en RoutIT) te detecteren en een andere route te selecteren als deze beschikbaar is.

Een voorbeeld van een back-up oplossing is een zakelijke DSL of Extended Ethernet verbinding en een Thuiswerkerlijn, waarbij al het verkeer over de zakelijke lijn loopt en bij een storing via de Thuiswerkerlijn. Ook is het mogelijk verkeer asynchroon te routeren en hierbij de upload en download van verschillende lijnen te combineren* (geen load-balancing!).

**Hiervoor moeten beide lijnen Zakelijk zijn.*

Border Gateway Protocol



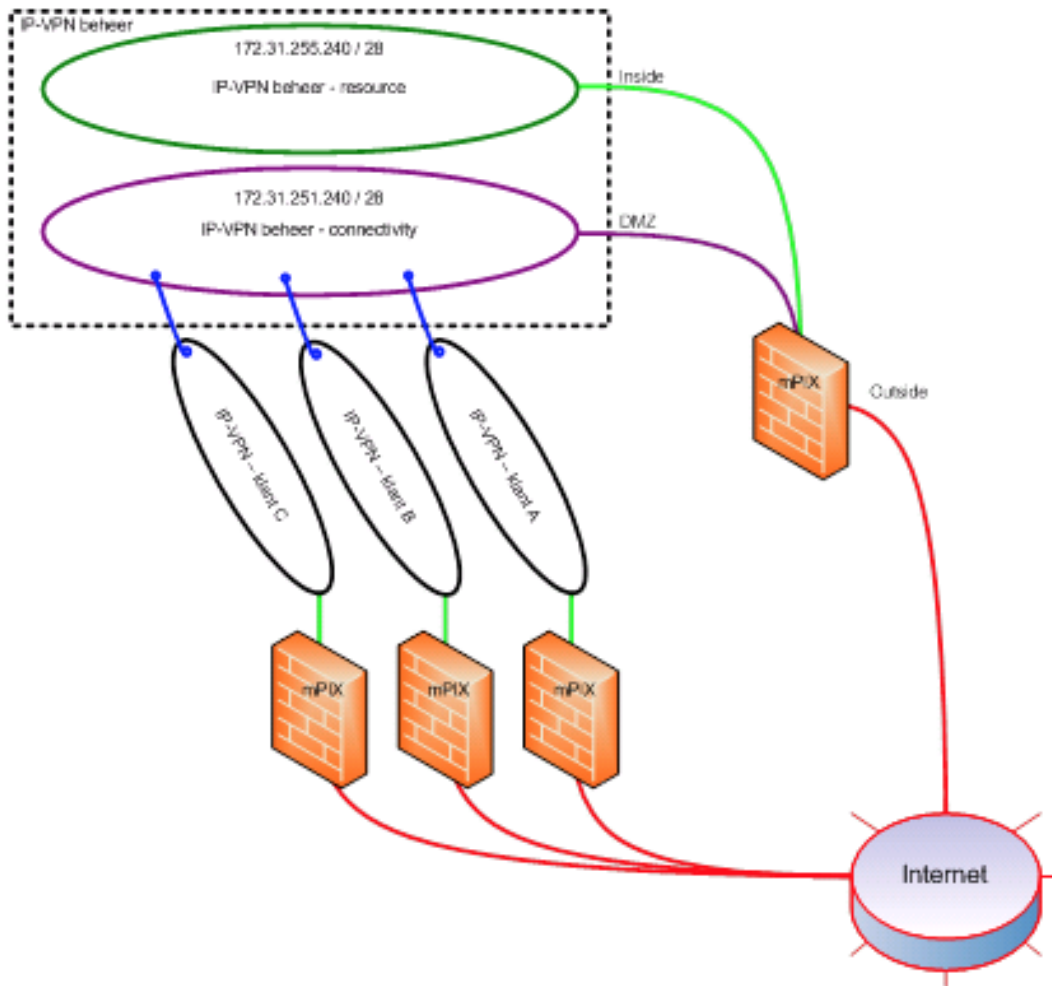
4 IP-VPN (Plus) Beheer (info t.b.v. CBG Connect)

Kenmerk IP-VPN (Plus) Beheer

De IP-VPN (Plus) Beheer zorgt ervoor dat de er volledig beheer kunt uitgevoerd kan worden uitvoeren bij uw klanten die een RoutIT IP-VPN hebben. Ook kunt u gemeenschappelijke diensten aanbieden aan uw individuele klanten binnen hun eigen IP-VPN. Elke IP-VPN behoudt in deze constructie zijn volledige onafhankelijkheid.

RoutIT IP-VPN beheer is in essentie een reguliere IP-VPN of IP-VPN Plus. Een IP-VPN (Plus) Beheer bestaat uit 2 delen: de resource IP-VPN (zichtbaar in IRMA) en een connectivity IP-VPN (niet zichtbaar in IRMA). Daarnaast is standaard een *mShield | Level Beheer* aanwezig.

In de resource IP-VPN worden de locaties of diensten van de CSP opgenomen. Bijvoorbeeld monitoring, terminal-oplossingen en antivirus oplossingen. Door de firewall tussen de resource IP-VPN en de connectivity IP-VPN is het mogelijk om verkeer van en naar de resource IP-VPN te limiteren. Alle verbonden klant IP-VPN's worden in de connectivity IP-VPN samengebracht. Een voorwaarde voor het gebruik van IP-VPN (Plus) Beheer is dat alle eindgebruiker locaties een uniek IP subnet hebben binnen de gehele oplossing.



Oplevering

RoutIT levert IP-VPN (Plus) Beheer standaard als volgt op:

- Verbonden klant IP-VPN's kunnen default niet naar de resource IP-VPN communiceren;
- De resource IP-VPN kan default wél naar de klant IP-VPN's communiceren.

U kunt deze configuratie na oplevering zelf wijzigen. Klant IP-VPN's kunnen nooit onderling communiceren.

Firewall

Om de IP-VPN (Plus) Beheer te ontsluiten naar het internet, dient een publieke WAN-interface (outside interface) op de mShield besteld te worden. Hiervoor dient u de standaard meegeleverde *mShield | Level Beheer* te upgraden naar Level 1, 2, 3 of 4. Deze mShield wordt vanaf dan separaat in rekening gebracht conform de tarieflijst van mShield. U kunt tijdens uw bestelling van IP-VPN (Plus) Beheer ook direct kiezen voor deze levels, om uw mShield direct van een outside interface te voorzien.

Vershil IP-VPN Beheer & IP-VPN Plus Beheer

Het verschil tussen een IP-VPN Beheer en IP-VPN Plus Beheer is dat u in de laatste, net zoals in een IP-VPN plus, in de resource IP-VPN gebruik kunt maken van BGP om redundante verbindingen en/of meerdere netwerken per locatie mogelijk te maken.

5 IP-VPN Voice

P-VPN Voice bevat vele voordelen van de standaard IP-VPN, maar is specifiek ingericht voor klanten met een HIP of KPN ÉÉN telefooncentrale.

Met de IP-VPN Voice biedt u uw klant een veilige netwerkomgeving voor telefoniediensten. Dankzij de standaard ontsluiting voor autoprovisioning is bij IP-VPN Voice geen additionele firewall (mShield) bestelbaar maar kunnen toestellen wel via het RoutIT netwerk profielen ophalen.

U kunt IP-VPN Voice toepassen voor één HIP of KPN ÉÉN telefooncentrale/groep. Slechts één VoIP-domein van de telefooncentrale kan zich registreren bij de RoutIT SBC.

Dit alles maakt de IP-VPN Voice een ideale oplossing voor uw klant met hosted telefonie, tegen een zeer scherp tarief.



Randvoorwaarden

IP-VPN Voice kent de volgende gebruiksvoorwaarden:

- Per IP-VPN Voice is één HIP of KPN ÉÉN groep toegestaan;
- Per IP-VPN Voice is één klant toegestaan;
- Per IP-VPN Voice koppelt u maximaal 10 verbindingen (30 routes) van één klant;
- Ontsluiting naar de HIP/KPN ÉÉN autoprovisioning-servers en RoutIT NTP-servers is standaard inbegrepen;
- Geen internettoegang toegestaan vanuit/via IP-VPN Voice;
- Parent-Child constructie geldt niet voor IP-VPN Voice;
- Geen ondersteuning voor BGP.

6 IP-VPN Parent-Child

De IP-VPN Parent-Child constructie maakt het mogelijk diensten van 2 verschillende partners te combineren.

Bijvoorbeeld: *Partner A biedt de verbinding aan en Partner B biedt VoIP aan*

- Partner B heeft een dienst (VoIP) die hij/zij beschikbaar wil stellen voor klanten. Deze dienst is beschikbaar binnen de IP-VPN (Parent) van Partner B.
- Partner A heeft een verbinding bij Klant X en koppelt deze verbinding aan de IP-VPN (Child), waarbij Partner B de IP-VPN bezit (Parent).

Op deze manier is het mogelijk Klant X de producten m.b.t. de verbinding te laten afnemen bij Partner A en de producten m.b.t. VoIP te laten afnemen bij Partner B.

Let op: bestel altijd een nieuwe IP-VPN als Child. Bestaande IP VPN's kunnen niet worden geconfigureerd als Child van een andere (bestaande) Parent IP VPN. IP-VPN Voice kan niet als Parent of Child worden gebruikt.

7 BGP

U kunt BGP toepassen om redundantie te creëren op de klantlocatie, waarbij u over minimaal twee verbindingen beschikt. U kunt dit op twee manieren inrichten:

Active/Passive: De secundaire verbinding staat 'standby' om alle taken van de primaire verbinding over te nemen. Hierbij adverteert RoutIT in beide BGP-sessies de default gateway (0.0.0.0/0). Door middel van configuratie in de CPE wordt bepaald wat de hoofd- en backupverbinding wordt.

Active/Active: De primaire en secundaire verbinding worden gelijktijdig gebruikt. Bijvoorbeeld om data- en voiceverkeer gescheiden af te handelen. Bij onderbreking van één van de verbindingen, wordt al het verkeer over de tweede verbinding gerouteerd. Bij Active/Active adverteert RoutIT alle aanwezige netwerken in de IP VPN. Deze zullen dan in het CPE moeten worden gefilterd.

Daarnaast maakt BGP het mogelijk meerdere netwerken te adverteren.

Specificaties en vereisten

- De in BGP geadverteerde netwerken mogen groter zijn dan /24
- Verbindingen uit het Zakelijk portfolio zijn geschikt voor BGP. In geval van redundantietoepassing mag één van de verbindingen uit het Thuiswerker portfolio komen.
- BGP is toe te passen in combinatie met een IP-VPN Plus (Open).
- De verbinding moet over een /32 IP-adres beschikken.
- Maximaal 25 subnets per locatie.
- Alleen private IP reeksen in een IP VPN Plus (RFC1918).
- CPE met BGP-ondersteuning

Verbindingen

- **Verschillende netwerkleveranciers**
- Door verbindingen te bestellen bij verschillende RoutIT-netwerkleveranciers bereikt u de meest optimale vorm van redundantie en bent u niet afhankelijk van één telco/leverancier en neemt de kans op een single point of failure verder af.
- **Mobiel**
Met behulp van een 3G-router en de diensten Mobile Connect & Mobile GRE Tunnel kunt u een secundaire verbinding via het 3G-netwerk aanbieden aan uw klant.
- **Zelfde netwerkleverancier**
Indien u kiest voor twee verbindingen van dezelfde netwerkleverancier dient direct na bestelling van de secundaire verbinding een ticket aangemaakt te worden én direct telefonisch contact opgenomen te worden met de leverdesk voor verbindingen. Hierin geeft u aan dat de verbinding voor BGP gebruikt wordt en deze bij voorkeur op een ander handoverpoint dient uit te komen dan de primaire verbinding. Vermeld hierbij dus ook het orderID van de primaire verbinding. Indien u dit na oplevering van de secundaire verbinding doorgeeft, worden de aanpassingen uitgevoerd tegen de standaard modificatiekosten.

BGP Aanvragen

Een BGP configuratie op een verbinding kan aangevraagd worden door een ticket in te schieten op de betreffende verbinding. Voor elke verbinding waarvoor BGP benodigd is maakt u een ticket aan. De configuratie voor BGP wordt uitgevoerd zodra de verbinding actief is.

RoutIT Support heeft de volgende gegevens nodig, die u in uw ticket aangeeft:

- Voorgesteld ASN
- Voorgesteld BGP wachtwoord
- Gewenste configuratie (Active/Active, Active/Passive of Meerdere netwerken adverteren)
- OrderID van de tweede verbinding (indien van toepassing)

8 Verantwoordelijkheden CPE en SLA

Verantwoordelijkheden CSP

Omdat een RoutIT IP-VPN volledig van het internet gescheiden is, kan de CSP zelf haar private (RFC 1918) IP-nummerplan bepalen. De CSP kan dus de klant zonder om te nummeren of NAT te gebruiken alle klantlocatie koppelen. Meerdere IP-VPN's zouden dezelfde adressen kunnen gebruiken, maar wordt uit oogpunt van groei/uitbreiding afgeraden.

Doordat de IP-VPN volledig is afgesloten, kan de CSP zoveel private IP-adressen gebruiken als noodzakelijk is. De RoutIT IP-VPN blijft volledig transparant.

CPE klantomgeving

In de RoutIT IP-VPN wordt de meeste intelligentie geregeld door de RoutIT routers of de mShield. De routers op locatie hoeven alleen maar datapakketten te forwarden. Het voordeel hiervan is, dat de eindgebruiker geen dure IPSEC of firewall software/hardware dient aan te schaffen.

RoutIT adviseert om uitsluitend Cisco routers te gebruiken.

SLA

Deze dienst is beschikbaar in de volgende Service Level Agreements:

Dienst	SLA B	SLA N	SLA A
IP-VPN		X	

Service Level Agreements

Een Service Level Agreement (SLA) is een overeenkomst tussen opdrachtgever en opdrachtnemer waarin de afspraken over het niveau van de dienstverlening zijn vastgelegd.

Meldingen werkzaamheden en storingen

Werkzaamheden met impact op de beschikbaarheid van de dienst worden altijd gemeld op de website <http://www.cspreporter.nl/>. Deze website is publiekelijk beschikbaar. Indien mogelijk streeft RoutIT ernaar de melding tenminste 7 dagen voor de werkzaamheden te publiceren.

Levertijd

RoutIT IP-VPN producten kennen een levertijd van 1-2 werkdagen.

9 Algemene kaderzetting van deze dienstbeschrijving

Deze dienstbeschrijving vormt een onlosmakelijk deel van de ondertekende offerte in combinatie met Algemene Voorwaarden CBG Connect, de Algemene Voorwaarden Service Provider RoutIT en mogelijke bedrijfsspecifieke voorwaarden en afspraken en productbrochures.

De informatie in deze dienstbeschrijving is gelijk aan de informatie van Service provider RoutIT

CBG Connect behoudt zich het recht voor deze dienstbeschrijving zonder voorafgaande melding te wijzigen.

De dienstbeschrijving is uitsluitend bestemd voor intern gebruik binnen uw organisatie. Het maakt onderdeel uit van het contract tussen u en CBG Connect. Het document is aan u verstrekt om een afgewogen keuze te kunnen maken voor CBG Connect als leverancier van deze dienst.

Alle rechten met betrekking tot dit document zijn voorbehouden aan CBG Connect. Niets uit deze publicatie of delen ervan mag op enigerlei wijze worden gereproduceerd, toegankelijk gemaakt in een database of op andere wijze aan derden beschikbaar worden gesteld, tenzij CBG Connect hier op uitdrukkelijk verzoek van uw bedrijf schriftelijk toestemming voor heeft verleend.

Wijzigingen en typfouten voorbehouden.

CBG Connect B.V., januari 2017