interforce | uw ICT partner

IP-VPN

IP-VPN

Inhoudsopgave

HOOFDSTUK 1

1. dienstenbeschrijving

1.1 Introductie

Door het inzetten van MPLS binnen het Interforce Networks BV netwerk, is het netwerk optimaal te gebruiken voor gecombineerde diensten zoals data, voice en video. Bekende namen van deze diensten zijn triple-play en IP-NGN (IP-next Generation Network).

Binnen het Interforce Networks BV MPLS netwerk is het hierdoor mogelijk MPLS IP-VPN's te creëren. Deze IP-VPN's zijn technisch gezien gescheiden routeringstabellen op de routers binnen het Interforce Networks BV netwerk. Voor iedere klant wordt een apart label (uniek kenmerk) aan een IP pakket toegevoegd. Hierdoor is het mogelijk om op basis van het label en bijbehorende route unieke beslissingen te maken en voor iedere IP-VPN een "eigen" routeringtabel aan te leggen.

Klanten kunnen hierdoor heel eenvoudig een gescheiden of gesloten klantnetwerk creëren. Door gebruik te maken van een WAN netwerk zonder aanpassingen op locaties of ingewikkelde IP-SEC oplossingen aangeboden krijgen welke precies aansluiten aan hun wensen.

Wat is een IP-VPN?

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

Een Interforce Networks BV IP-VPN is volledig afgescheiden van het internet. Dit houdt in dat de dienste geheel gesloten wordt aangeboden. De Interforce Networks BV MPIX firewall ontsluit alle vestigingen binnen de IP- VPN naar het internet. Deze Firewall wordt centraal beheerd voor alle vestigingen binnen de IP-VPN en zorgt voor de CSP wordt beheerd.

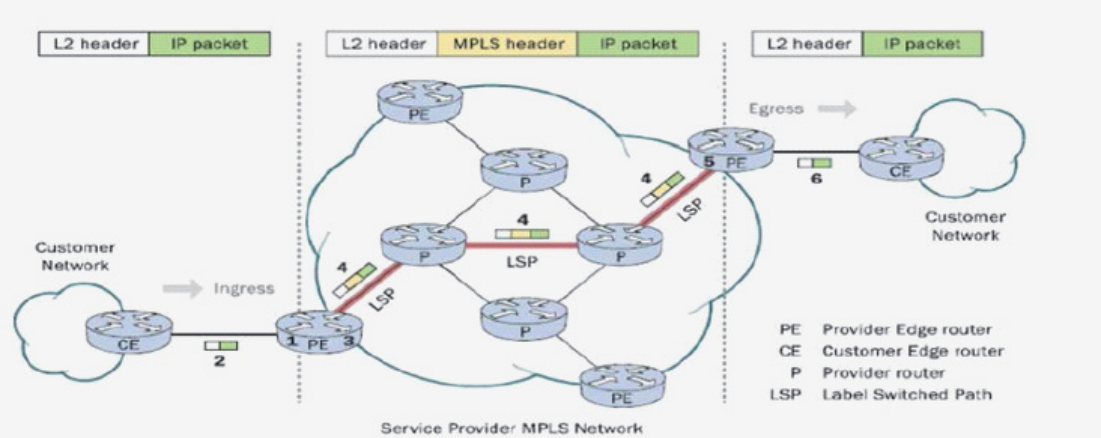
De klantlocaties worden binnen een IP-VPN permanent met elkaar verbonden door middel van de Interforce Networks BV wereldwijde MPLS backbone. Deze dienst maakt dus geen gebruik van het internet als transportmedium. De beveiliging van de data is verzekerd, dit omdat het dataverkeer het Interforce Networks BV 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. Indien gewenst kunnen er prioriteiten toegekend worden aan verschillende typen dataverkeer (Class of Service/ Quality of Service, zie hiervoor ook de QoS dienstenbeschrijving).

IP-VPN is de oplossing voor alle bedrijfskritische en/of tijdskritische applicaties.

1.1.2. hoe werkt het MPLS-netwerk?

Om de werking van een MPLS-netwerk te demonstreren, volgen we de datastroom door het netwerk in de onderstaande afbeelding:

- In het MPLS-netwerk worden tussen de PE-routers en de P-routers, LSP's opgesteld (label Switched Path).
- Vanuit het versturende klantnetwerk wordt er niet MPLS-verkeer (DSL, Ethernet, ect.) verzonden, door de Ce-router, naar de Ingress (inkomend) PE-router aan de rand van het MPLS-netwerk.
- De PE-router koppelt het IP pakket aan een IP-VPN (FEC) en voegt de juiste MPLS-labels toe aan het pakket. Het pakket wordt via de LSP geswitched (elke tussenliggende P-router verwisselt labels zoals opgegeven door de informatie in de LIB om het pakket naar de volgende stap te switchen).
- Bij de Egresse-PE wordt het laatste MPLS-label verwijderd en wordt het IP pakket doorgestuurd via de traditionele routingmechanismen.
- Het IP pakket komt binnen op de CE en is afgeleverd op het ontvangende klantennetwerk.



1.1.3 Interforce Networks BV IP-VPN kenmerken

	IP-VPN	IP-VPN+	IP-VPN(+) open
Diensten	Alle	Alle	Alle
IP addressen	Private (rfc1918)	Private (rfc1918)	Publiek
Max IP addressen[1]	256	-	-
Connectivity	Alleen PPP	PPP + routering	PPP + routering
Redundancy	Geen	BGP + EiGRP	BGP + EiGRP
mPIX	v	v	v
mPIX +	v	v	v
mSSL	v	v	x
mVPN telewerk	v	v	x
Colocatie	v	v	v
Blades	v	v	v

Interforce Networks BV IP-VPN heeft de volgende kenmerken:

- Een transparant geïntegreerd netwerk.
- Keuze uit meerdere leveranciers (BBned, Versatel, KPN….).
- Een ruim assortiment van verbindingen.
- Centraal beveiligde internettoegang vanuit de Internet Networks BV-backbone.
- Redundant en loadbalanced verbindingen.
- Verkeer dynamisch te routeren.
- Back up verbinding (bv DSL of BGP).
- Thuiswerkers te koppelen door mSSL en/of mVPN groep.
- Layer 2 Class of Service mogelijk.
- Layer 3 Quality of Service mogelijk.
- Service level Agreements.
- Eenvoudige integratie van Colocatie diensten.
- Eenvoudig beheer door Interforce Networks BV IP-VPN Beheer.
- Zorgvuldige implementatie en begeleiding bij klantconfiguraties d.m.v. voorbeeld scrips.

1.2 IP-VPN

Met Interforce Networks BV kan de CSP eenvoudig en op veilige wijze een of meerder bedrijfsnetwerken, bedrijfslocaties en thuiswerkers verbinden tot een privénetwerk. Hiermee is de CSP in staat om het MKD een passende oplossing te bieden, waarbij hoge investeringen voor de eindgebruiker uitblijven.

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 CE router (klantlocatie). Er is geen dynamische communicatie mogelijk tussen het klantennetwerk en het Interforce Network BV IP-VPN.

Hierdoor is het niet mogelijk een redundancy oplossing te maken waarbij beide lijnen, tegelijk actief zijn (PPP link). Tevens is het niet mogelijk meer dan 256 IP adressen (wel op zakelijke- en SMB verbinding) op 1 lijn te plaatsen, standaard zijn dit er maximaal 16, meer zijn mogelijk, uitsluitend op aanvraag.

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 CE (klant router) en wordt niet actief ondersteund door Interforce Networks BV.

Interforce Networks BV staat toe dat voor de stand-by lijn een Home wordt gebruikt die op het moment van een failover of back-up situatie wel het subnet routeert als de andere lijn een zakelijke of SMB lijn is.

Door het standaard gesloten karakter van een IP-VPN is het standaard niet mogelijk het internet te benaderen. Om het internet te benaderen is een firewall op locatie, op de colc of een Interforce Networks BV mPIX of mPIX+ dienst noodzakelijk. Zo kunnen alle aangesloten diensten via een centrale firewall naar het internet.

1.3 IP-VPN open

Met Interforce **IP-VPN open** kan de CSP eenvoudig en op veilige wijze een of meerdere bedrijfsnetwerken, bedrijfslocaties en thuiswerkers verbinden tot 1 publiek netwerk. Hiermee is de CSP in staat om het MKB een passende oplossing te bieden, waarbij hoge investeringen voor de eindgebruiker uitblijven.

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

Hierdoor is het niet mogelijk een redundancy oplossing te maken waarbij beide lijnen, tegelijk actief zijn (PPP link). Tevens is het niet mogelijk meer dan 256 ip adressen (wel op zakelijke- en SMB verbindingen) op lijn te plaatsen, standaard zijn dit er maximaal 16, meer zijn mogelijk, uitsluitend op aanvraag.

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 oplossingen kan alleen ingesteld worden op de CE (klantrouter) en wordt niet actief ondersteund door Interforce Network BV.

Interforce Networks BV staat toe dat voor de stand-by lijn een ADSL Home wordt gebruikt die op het moment van een failover of backup situatie wel het subnet routeert als de andere lijn een zakelijke of SMB lijn is.

Bijzonder aan deze vorm is dat deze **IP-VPN open** alleen uit publieke IP's bestaat en hierdoor geen firewall nodig heeft (wat eventueel wel mogelijk is). Het is bijvoorbeeld mogelijk om een IP-VPN af te nemen waarin publieke (niet Interforce Networks BV) IP adressen gebruikt worden welke via een colo verbinding afgeleverd worden. Hierdoor ontstaat een onzichtbaar netwerk voor de klant en kan een partnet een "eigen" infra tonen.

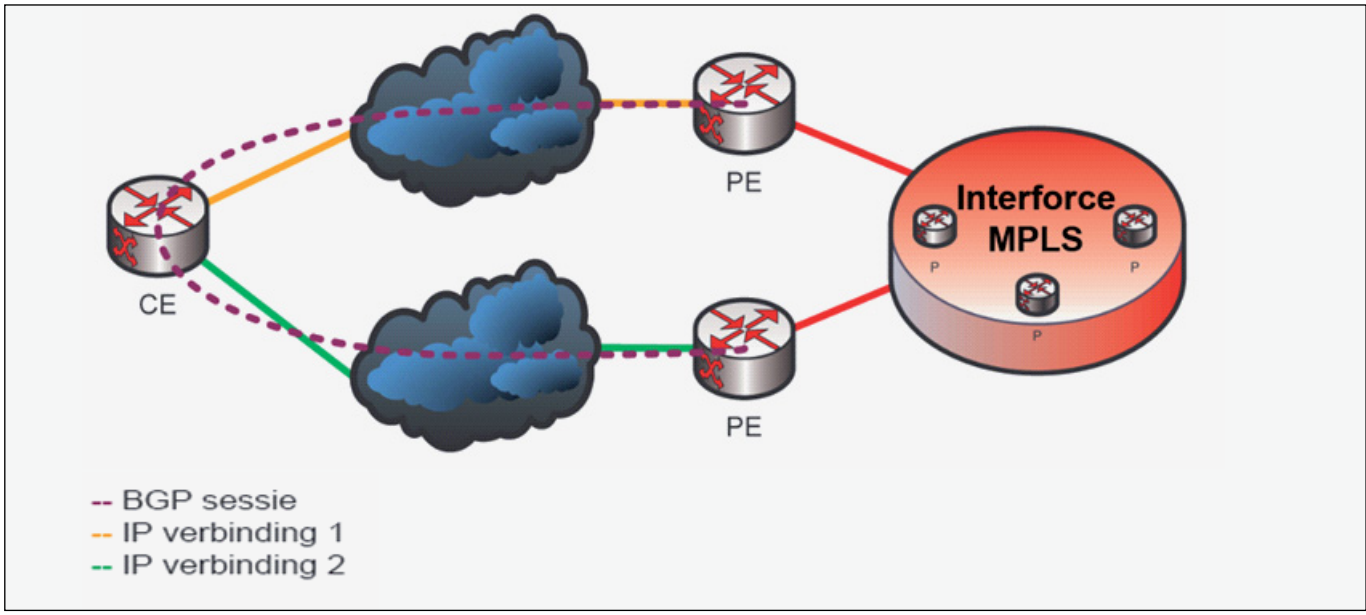
1.4 IP-VPN plus

Het Interforce Networks BV **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 of load-balancing toe te passen.

Er worden 2 routerings protocollen ondersteund;

BGP, geschikt om meerdere subnets te transporteren en voor redundancy.

Via het BGP (Border Gateway Protocol) 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 CE op klantlocatie kan bepalen wat er met de routes moet gebeuren (zowel inkomend als uitgaand). Iedere BGP sessie bestaat uit 2 TCP sessies, waardoor het mogelijk is om storingen in de onderliggende domeinen (klant, telco en Interforce Networks BV) 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 ADSL Home, waarbij al het verkeer over de zakelijke lijn loopt en bij een storing via de ADSL Home. Ook is het mogelijk verkeer asynchroon te routeren en hierbij de upload en download van verschillende lijnen te combineren (geen load-balancing!).

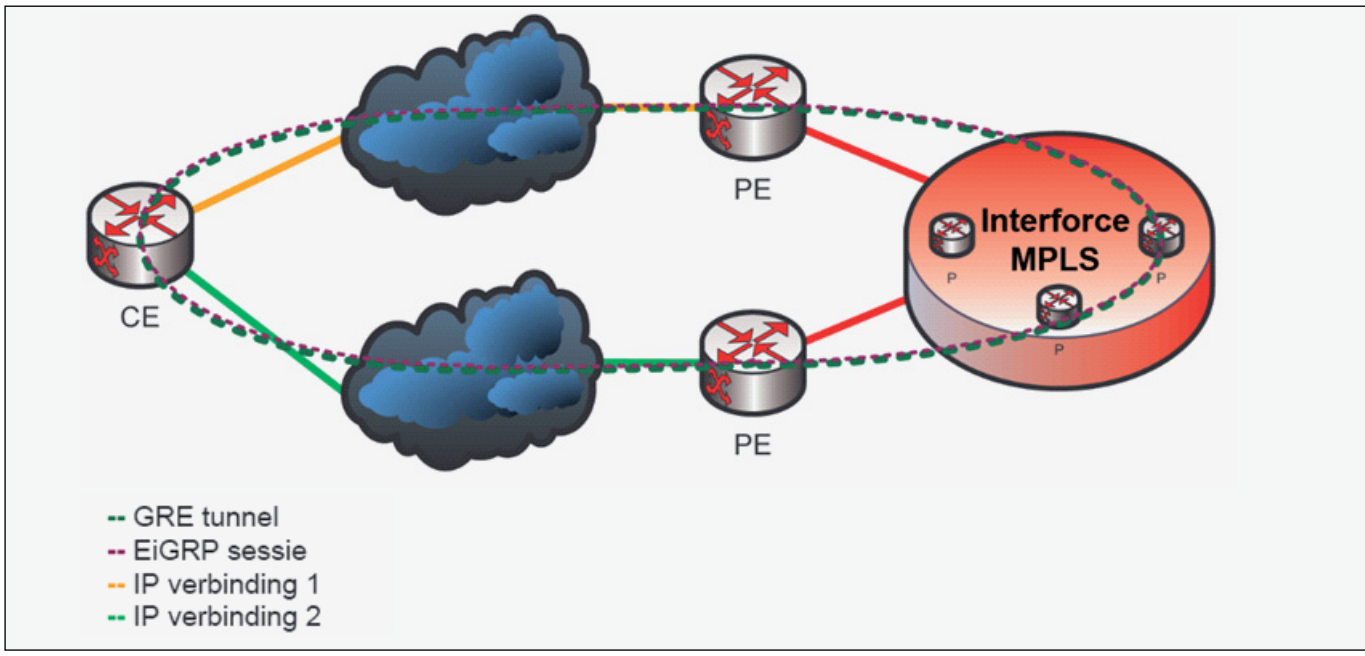


EiGRP, geschikt om load-balancing toe te passen.

Via het Cisco EiGRP protocol is het mogelijk meerdere zakelijke lijnen te combineren en hiervoor load-balacing te activeren. Voor iedere verbinding wordt een GRE tunnel opgebouwd naar een centrale router van Interforce Networks BV, op deze GRE tunnel zal de bandbreedte van de onderliggende lijn geconfigureerd worden. Hierdoor is het mogelijk om op basis van de 5 K waardes van EiGRP (bandwidth, Delay, Reliability, load MTU) over maximaal 6 paden load-balancing te activeren.

Interforce Networks BV staat toe dat voor de stand-by lijn een Telewerklijn wordt gebruikt die op het moment van een failover of bavk-up situatie wel het subnet routeert als de andere lijn een zakelijke of SMB lijn is. Dit geldt alleen in een stand-by configuratie, niet bij een load-balanced configuratie dan moeten beide lijnen zakelijke of SMB lijn zijn.

Door het standaard gesloten karakter van een IP-VPN is het standaard niet mogelijk het internet te benaderen. Om het internet te benaderen is een firewall op locatie, op de colo of een Interforce Networks BV mPIX of mPIX+ dienst noodzakelijk. Zo kunnen alle aangesloten diensten via een centrale firewall naar het internet.



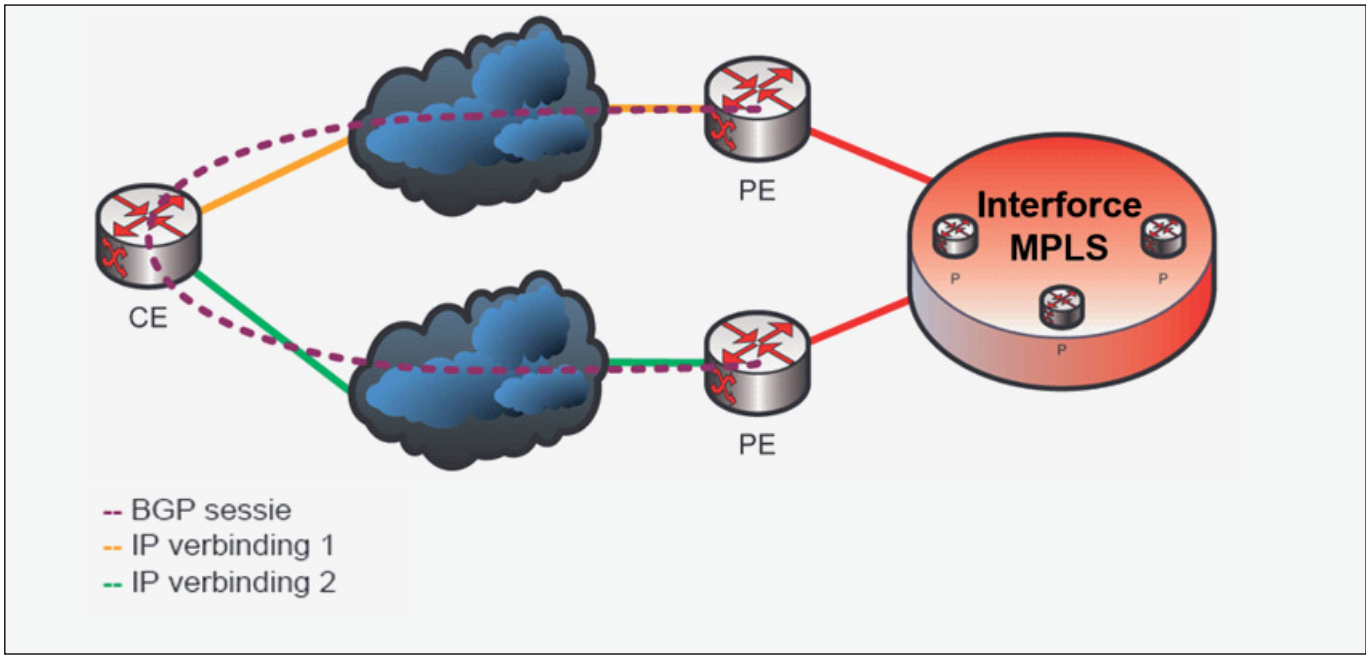
1.5. IP-VPN plus open

Het interforce Networks Bv **IP-VPN Plus open** bevat alle eigenschappen van een IP-VPN open 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 of load-balancing toe te passen.

Er worden 2 routerings protocollen ondersteund;

BGP, geschikt om meerdere subnets te transporteren en voor redundancy.

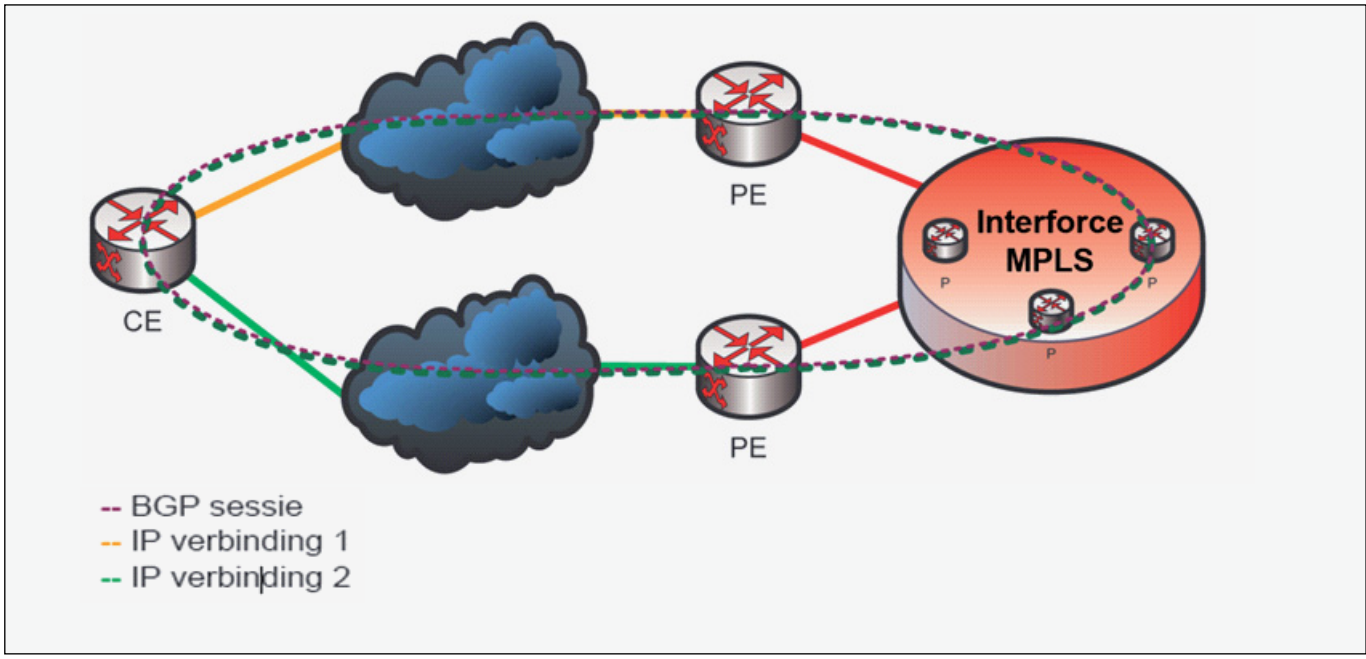
Via het BGP (Border Gateway Protocal) is het mogelijk om routes uit te wisselen en tevens extra attributen per route mee te geven. Hierdoor is het mogelijk om voorrang aan bepaalde routes te geven waardoor de CE op klantlocatie kan bepalen wat er met de routes moet gebeuren (zowel inkomend als uitgaand). Iedere BGP sessie bestaat uit 2 TCP sessies, waardoor het mogelijk is om storingen in de onderliggende domeinen (klant, telco en interforce Networks BV) 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 ADSL Homelijn, waarbij al het verkeer over de zakelijke lijn loopt en bij een storing via de ADSL Homelijn. Ook is het mogelijk verkeer asynchroon te routeren en hierbij de upload en download van verschillende lijnen te combineren (geen load-balacing!).



EiGRP, geschikt om load-balancing toe te passen.

Via het Cisco EiGRP protocol is het mogelijk meerdere zakelijke lijnen te combineren en hierover load-balancing te activeren. Voor iedere verbinding wordt een GRE tunnel opgebouwd naar een centrale router van Interforce Networks BV, op deze GRE tunnel zal de brandbreedte van de onderliggende lijn geconfigureerd worden. Hierdoor is het mogelijk om op basis van de 5K waardes van EiGRP (Bandwidth, Delay, Reliability, Load, MTU) over maximaal 6 paden load-balancing te activeren.

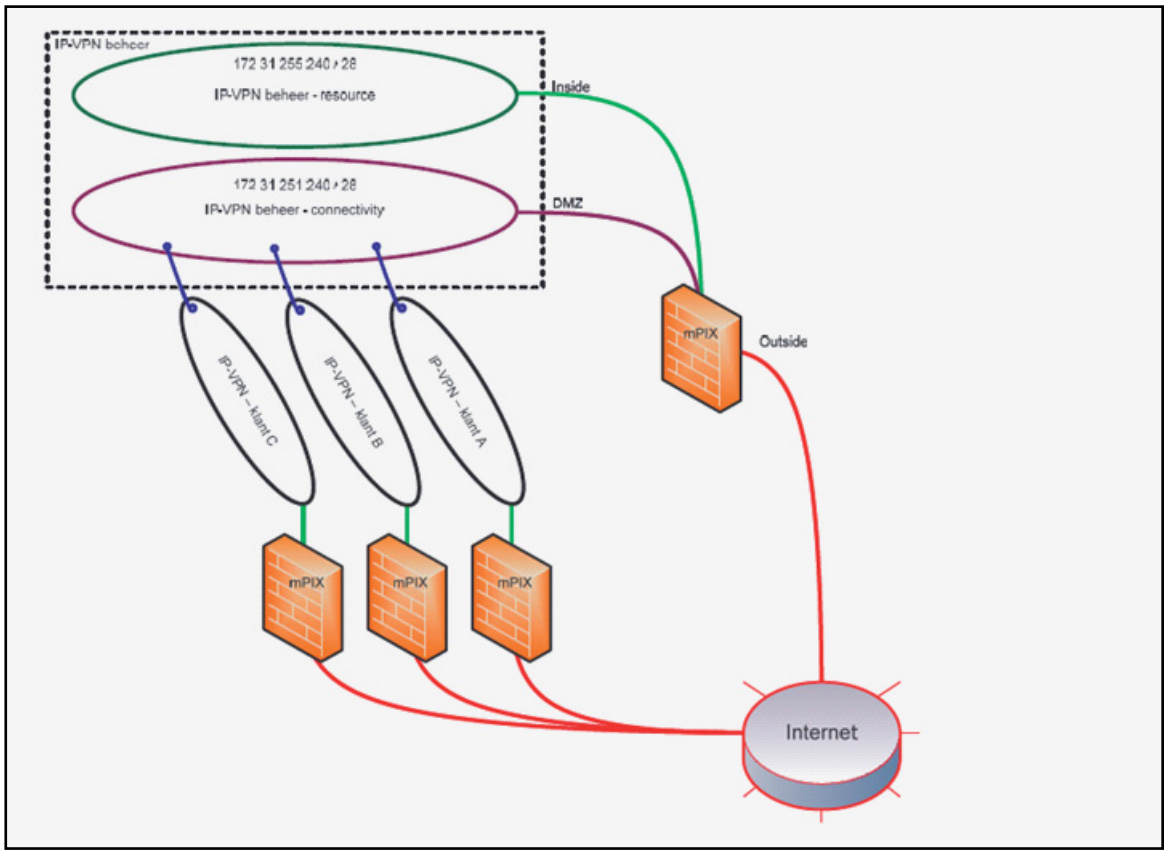
Bijzonder aan deze vorm is dat deze IP-VPN plus open allen uit publieke IP's bestaat en hierdoor geen firewall nodig heeft (kan eventueel wel). Het is als voorbeeld mogelijk om een IP-VPN af te nemen waarin publieke IP adressen gebruikt worden welke direct met het internet verbonden zijn en toch gebruik te maken van automatische redundancy op klant locatie.



1.6 IP-VPN (plus) beheer

Met Interforce Networks BV **IP-VPN beheer/IP-VPN plus beheer** is het voor de CSP mogelijk volledig beheer uit te voeren bij meerdere klanten die een Interforce Networks BV IP-VPN hebben, dit terwijl iedere IP-VPN zijn volledige onafhankelijkheid bewaart.

Interforce Networks BV beheer is in essentie een "gewone" IP-VPN of IP-VPN plus. Een IP-VPN beheer bestaat uit 2 delen, de resource IP-VPN (zichtbaar in IRMA) en een connectivity IP-VPN worden de locaties of dienste van de CSP opgenomen, voorbeelden zijn monitoring, terminal oplossingen en antivirus oplossingen. Door de firewall tussen de twee IP-VPN te limiteren. Alle verbonden klant IP-VPN's worden in de connectivity IP-VPN samengebracht en kunnen wel naar de resource IP-VPN. Maar niet onderling communiceren.



Behalve de eigen verbindingen worden in Interforce Networks BV IP-VPN beheer ook de netwerken van uw klanten bekend gemaakt en in de IP-VPN's van de klanten wordt ook het IP-VPN beheer bekend gemaakt.

Met deze mogelijkheid maakt Interforce Networks BV het mogelijk om volledig beheer uit te voeren bij meerdere klanten die een Interforce Networks BV IP-VPN hebben, terwijl iedere IP-VPN zijn volledige onafhankelijkheid behoudt.

Een voorwaarde voor het gebruik van IP-VPN beheer is dat alle eindgebruiker locaties uniek genummerd zijn. Het Interforce Networks BV beheer moet alle normale IP-VPN's kunnen onderscheiden.

1.7 welke SLA geldt voor IP-VPN diensten?

Een service level Agreement is een contract over het te leveren niveau en type service. Vervolgens wordt bijgehouden of de klant ook daadwerkelijk krijgt waar hij voor betaalt. Een SLA wordt o.a. opgesteld voor een organisatie die een deel van de automatisering wil uitbesteden aan een leverancier. Interforce Networks BV levert bij Interforce Networks BV IP-VPN, een SLA (N)ext Business Day.

SLA N	SLA Next Business Day 99,6% beschikbaarheid
U kunt iedere werkdag (maandag t/m vrijdag) tussen 09.00 en 17.00 uur een incident bij de supportdesk melden. Response tijd < 4uur. Het incident wordt dan maximaal de volgende werkdag hersteld. BBned geeft de gegarandeerde Service Levels alleen op het DSL netwerk, niet op de local loop (oftewel de koperdraad van de wijkcentrale naar het aansluitadres). De richtlijn voor het herstel van het koperdraad is 80% binnen 24 uur, 90% binnen 48 uur.	

HOOFDSTUK 2

2. Technische Specificaties van de Interforce Networks BV IP-VPN Dienst

Dit document beschrijft de technische specificaties van de Interforce Networks BV IP-VPN oplossing.

De volgende onderwerpen vindt u terug in dit document:
- Netwerk structuur; MPLS IP-VPN
- Verantwoordelijkheden CSP
- Interforce Networks BV opties;
- End-user omgeving

2.1 MPLS-VPN

Aan de basis van het Interforce Networks BV IP-VPN staat het MPLS-VPN protocol. MPSL staat voor Multiple Label Switching.

MPLS IP-VPN werkt op basis van labels die toegevoegd worden aan data pakketten. De bestemming van een pakket wordt niet meer op basis van IP-adres gedefinieerd, maar op basis van het label.

Door deze toevoeging is het IP- adressen kunnen overlappen. Immers: IP-adres 192.168.10.1 label 50 is nu een ander adres dan 192.168.10.1 label 60.

Ook het versturen van verkeer tussen routers gaat op basis van labels, niet meer op basis van IP- adressen. Iedere dienst krijgt zijn eigenlabel, voor Interforce Networks BV

MPIX een label, voor Interforce Networks BV colocatie een label ect. Deze labels worden voor het IP-VPN label geplaatst. Wanneer een pakket dus van VPN 50 op de Interforce Networks BV zakelijk DLS router van VPN 50 op de colocatie moet, wordt eerst het VPN 50 label aan het pakket geplakt, en daarna het bestemmingslabel “colocatie”.

Schematisch ziet het er als volgt uit:

Bestemmings-tabel	VPN label	Datapakket

Het voordeel is dat bij het versturen van een datapakket bekent is wat de eindbestemming is en welk pad genomen moet worden. Normaal moeten alle apparaten tussen bron en bestemming afzonderlijk bepalen welk pad er genomen moet worden, nu is dat aan de hand van het tabel vooraf al bepaald. Dit zorgt voor snellere doorvoer in het IP-VPN netwerk.

Wanneer een datapakket aankomt bij de bestemmings router wordt het bestemmingstabel eraf gehaald. Daarna wordt er naar het IP-VPN label gekeken. Aan de hand van dit tabel wordt het datapakket naar het juiste IP-VPN gestuurd. In dit IP-VPN wordt het datapakket aan de hand van bestemmingsadres doorgestuurd naar de juiste DLS aansluiting, server, of Andere dienst.

2.2 verantwoordelijkheden CPS

Omdat een Interforce Networks BV 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 kunnen dezelfde adressen gebruiken. Mits er geen gebruik gemaakt wordt van IP-VPN beheer dienst van Interforce Networks BV. zolang binnen een IP-VPN alle vestigingen als noodzakelijk is. De Interforce Networks BV IP-VPN blijft volledig transparant.

2.3 End-user omgeving

In de Interforce Networks BV IP-VPN wordt de meeste intelligentie geregeld door de Interforce Networks BV routers of de MPIX. 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.

Interforce Networks BV adviseert om uitsluitend Cisco routers te gebruiken. Ondersta-ande Cisco routers worden veel gebruikt.

2.3.1 De Cisco SB 100 serie

De Cisco SB series router is een eenvoudige router met weinig extra mogelijkheden en een daar bij passend laag prijspeil. Deze router is ideaal voor eenvoudige vestigingen waar bijvoorbeeld QoS of meerdere verbindingen geen rol spelen. Deze router is niet geschikt voor adsl2+

2.3.2 De Cisco 850 serie

De 850 serie is een router voor het MKB-segment van Cisco. De 850 serie heeft alle functionaliteiten in zich voor IP-VPN, beperkte QoS en geavanceerde beveiligingsfuncties. Deze router is ideaal voor eenvoudige vestigingen waar bijvoorbeeld QoS of meerdere verbindingen een mindere rol spelen. Deze router is ook geschikt voor adsl2+

2.3.3 De Cisco 870 serie

De 870 serie is de krachtigste router uit het MKB segment van Cisco. De 870 serie heeft alle functionaliteiten in zich voor IP-VPN plus, QoS en geavanceerde beveiligingsfuncties. Wanneer op een locatie QoS, dynamische routering of extra firewall/ ids functionaliteit gewenst is is deze router een geschikte kandidaat. Deze router is ook geschikt voor adls2+.

2.3.4 De Cisco 1800 routers

Wanneer meerdere verbindingen gestapeld worden, is de Cisco 1800 de meest gebruikte router. Door het gebruik van Wan Interface Cards (WIC's) kunnen verschillende soorten interfaces gecombineerd worden in een router.

Bijlage 1: Begrippenlijst

Onderstaande definities hebben dezelfde betekenis in zowel dienstenbeschrijving, algemene voorwaarden en de overeenkomst:

CSP	Contractant van Interforce Networks BV
Eindgebruiker	Contractant van CSP
ATM	Asynchronous Transfer Mode, technologie voor datacommunicatie
PVC	Permanent Virtual Circuit, data te transporteren over ATM
CPE	Router/ bridge bij de klant
IP-VPN	Gesloten virtual private netwerk
MPIX	Managed hosted Cisco PIX firewall
Interconnect	De connective van de aan het Interforce Networks BV- network gekoppelde telco's
SLA	Service Level Agreement
IS/RA	punt het lokale punt waar het koperdraad een gebouw binnenkomt..
QoS	Quality of Service