Dienstbeschrijving
mShield

RoutIT

Datum: 2014

Versielog RoutIT

Algemeen	31-07-2014
Levels, mPix& technische kenmerken	24-06-2016
Werking, kwaliteit & SLA	13-02-2014
Modificaties	19-02-2014
Technische specificaties	04-08-2014

Inhoudsopgave

1 Inleiding

De mShield dienst voorziet in de behoefte van bedrijven voor een centrale firewall oplossing. Deze oplossing is gebaseerd op technologie van Cisco en bevat de functionaliteit van een enterprise oplossing. mShield is een complete firewall tegen lage maandelijkse kosten. Daarnaast heeft u geen zorgen over updates, performance, licenties en hardware.

Wat is mShield?

mShield is een complete firewall die geheel door de CBG Connect in te stellen is. mShield kan gebruikt worden om een IP-VPN met het internet te verbinden, maar kan ook gebruikt worden om meerdere IP-VPN's of colocaties te koppelen. Het gebruik van mShield maakt het mogelijk om de beveiliging van uw netwerk(en) centraal te realiseren zonder de hoge kosten voor aanschaf van apparatuur.

mShield varianten

Volgende mShield varianten zijn beschikbaar.

- **mShield (Level 1 t/m 4)**
  Voor bedrijven die behoefte hebben aan een uitgebreide firewall op meerdere verbindingen die in één IP-VPN wolk zitten, biedt CBG Connect mShield aan. Deze mShield wordt geleverd in combinatie met een IP-VPN (zie Dienstbeschrijving IP-VPN, dient los te worden besteld). Deze dienst is leverbaar op alle IP VPN diensten waarin wederom de connectivity diensten zoals Fiber, ADSL, SDSL en Extended Ethernet beschikbaar zijn.
- **mShield Redundant (Level 1 t/m 4)**
  Idem als mShield. Deze firewall is redundant uitgevoerd.

2 Levels, mPIX & technische kenmerken

mShield Levels

mShield is beschikbaar in vier verschillende levels. De levels staan voor het pakket aan resources dat bij de betreffende uitvoering hoort. Onderstaande tabel biedt een overzicht van de eigenschappen van ieder level:

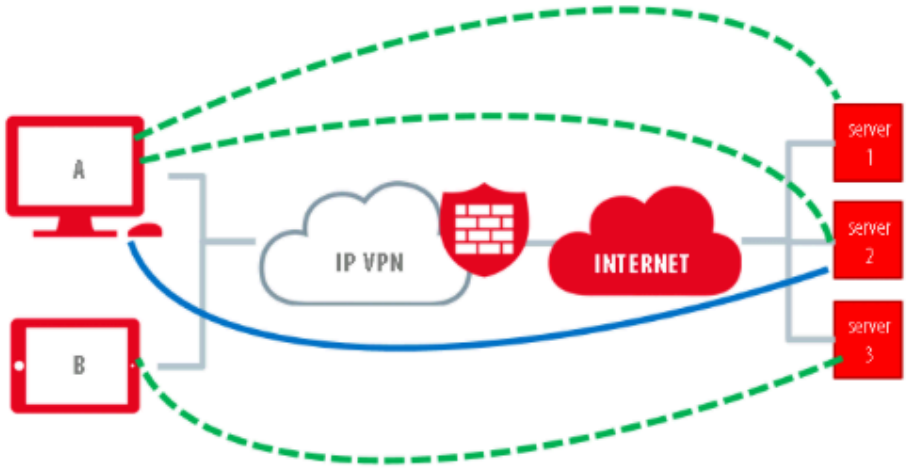
Resource	mShield Level 1	mShield Level 2	mShield Level 3	mShield Level 4
ASDM Sessies	2	2	2	2
SSH	2	2	2	2
Hosts	2000	3000	5000	10000
Connections	5000	12500	50000	100000
Xlates	5000	12500	50000	100000
Connections/sec	1000	2000	4000	8000
Syslog/sec	100	250	500	500
Static routes	25	100	200	500
Inspects/sec	100	250	500	500
IPsec tunnels	0	5	10	15
Interfaces	3	4	4	6
Bandbreedte*	10 Mb/s	20 Mb/s	40 Mb/s	80 Mb/s

* Gemiddelde waarde over de gehele maand op fair use basis.

3 Hosts, Xlates & Connections

Het inventariseren van de behoeften van uw klant is essentieel voor de keuze van het juiste mShield level. Belangrijk zijn onder andere het aantal benodigde hosts, xlates en connections.

- **Hosts**
  mShield telt één host per apparaat per connection, wanneer twee apparaten/servers verbinding met elkaar maken. Oftewel, minimaal 2 hosts voor één connection. Een gelijktijdige tweede verbinding tussen dezelfde twee apparaten/servers telt niet mee in de host-telling.
  Gaat het om bijvoorbeeld een website, dan dient u er rekening mee te houden dat er meer dan 2 hosts zijn bij de opbouw van de connection. Websites spreken vaak externe bronnen aan (bijvoorbeeld voor advertenties, afbeeldingen, video's). Dit zijn meerdere onderliggende connections, waarvoor ook steeds hosts geteld worden.
- **Connections**
  Zodra de verbinding is gerealiseerd en er een verkeersstroom actief blijft, tellen de eerder genoemde hosts mee in het totaal aantal bezette hosts. Een RDP-sessie is een voorbeeld van een actief-blijvende verbinding. Maar ook een website die continu informatie blijft ophalen.
- **Xlates (translaties)** Een xlate staat voor de vertaling van een publiek naar privaat IP-adres, en vice versa. Een xlate bestaat uit één of meerdere connections.
- **Voorbeeld**



- Er zijn 3 connectieverzoeken: van apparaat A naar Server 1 en Server 2, en van apparaat B naar Server 3
- De blauwe lijn is een gerealiseerde connectie met actieve verkeersstroom en telt ook mee in de host-telling.
- In dit voorbeeld is er sprake van minimaal 6 hosts

Interfaces

Aan een mShield kunnen meerdere interfaces worden toegekend. Standaard zijn dit er twee, inside en outside. Hier kan een extra interface aan worden toegekend voor bijvoorbeeld een DMZ of een voice IP-VPN. De interne interfaces kunnen in verschillende IP-VPN's zijn opgenomen. RoutIT ondersteunt maximaal het opgegeven aantal interfaces per mShield.

Verschillen mShield en MPix

In onderstaande tabel ziet u eenvoudig welke mPix vergelijkbaar is met de nieuwe mShield producten:

mPIX	mShield
mPIX VPN	mShield Level 1
mPIX Plus VPN	mShield Level 2
mPIX Redundant VPN	mShield Redundant Level 2

Raadpleeg de tabel met mShield-specificaties voor de exacte waarden die horen bij het gekozen level.

Technische kenmerken mShield

- Doorvoersnelheid van in totaal 10 Gbps
- Twee miljoen gelijktijdige sessies
- 125.000 nieuwe sessie's per seconde
- Native IPv6 ondersteuning in één beheer schil
- IPsec tunnels direct toepasbaar op mShield
- Per mShield meerdere interfaces mogelijk
  - Standaard inside en outside interface
  - Mogelijkheid tot extra interfaces
  - Per interface een IP-VPN
- Per mShield resource management (voorkomt dat 1 mShield alle resources verbruikt)
- Per interface inkomende en uitgaande security rules
- Webinterface (ASDM, Java applet)
- CMD line beheer mogelijk (SSH)
- SNMP
- Syslog (afhankelijk van mShield level).
- DoS bescherming
- Uitgebreide real time log viewer
- Time-based security policy
- Security policies tijdelijk op enabled of disabled zetten

Kenmerken mShield Redundant

mShield Redundant is een redundant uitgevoerde mShield. De redundantie houdt in dat:

- er twee instanties van de mShield actief zijn op twee verschillende machines;
- deze machines fysiek gescheiden zijn op twee verschillende colocaties;
- de configuratie van de Firewall eenmalig wordt uitgevoerd - deze wordt automatisch geactiveerd op beide instanties;
- als de primaire firewall module niet bereikbaar (i.v.m. onderhoud of storing) is, de secundaire firewall het overneemt.

4 Werking, kwaliteit & SLA

Werking mShield

Door het toepassen van een mShield is het mogelijk een IP-VPN te combineren met een complete firewall. mShield kan door CBG Connect zelf ingesteld worden en RoutIT hoeft alleen in de eerste opzet de toegang tot mShield te activeren. Hierdoor kunnen wijzigingen en toevoegingen direct en op ieder willekeurig moment van de dag doorgevoerd worden. De beleving van dit product is gelijk aan een lokale firewall, alleen zijn de investeringen en onderhoud hiervan de verantwoordelijkheid van RoutIT.

Kwaliteit mShield

Door het gebruik van hoogwaardige Cisco apparatuur is de kwaliteit van de dienst uitmuntend. Cisco heeft jarenlange expertise op het gebied van firewalls en heeft in deze markt een groot aandeel. De bewezen technologie Cisco is toegepast in de mShield module van RoutIT. Hierdoor en door het RoutIT backbone netwerk, is het mogelijk de dienst aan te bieden met de hoogste kwaliteit zoals deze van RoutIT verwacht mag worden. Het backbone netwerk van RoutIT wordt continu gemonitord en waar nodig wordt er (pro)actief gereageerd door RoutIT. Door deze monitoring kan RoutIT trends en analyses vergelijken en zodoende zorgen voor voldoende capaciteit.
Het grote verschil van mShield ten opzichte van andere oplossingen is dat er op klantlocatie geen extra apparatuur geplaatst hoeft te worden. Ook wordt al het verkeer door de firewall op een centrale locatie geleid en is het niet noodzakelijk iedere locatie te voorzien van een eigen firewall. Hierdoor heeft een IP-VPN wolk één security policy. Elke locatie behoudt zijn maximale download bandbreedte, omdat de verbinding van de mShield firewall naar het internet maximaal is.

SLA

Deze dienst is beschikbaar in de volgende Service Level Agreements:

Dienst	SLA B	SLA N	SLA A
mShield		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.
De RoutIT Service Level Agreements kunt u terug vinden in de dienstbeschrijving Service Level Agreements Voor vragen kan er contact opgenomen worden met CBG Connect B.V. 0228 56 60 70 of via verkoop@cbgconnect.nl

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

mShield producten kennen een levertijd van ongeveer 2 werkdagen.

5 Modificaties

Level modificatie

mShield kent meerdere levels die het aantal resources vertegenwoordigen. U kunt bij CBG Connect eenvoudig een up- en downgraden in resource-level aanvragen. De kosten voor aanpassing van het level kunt u opvragen bij CBG Connect. Dit geldt ook voor een upgrade van mPIX VPN of mPIX VPN plus naar een mShield product (non-redundant).
Bij modificaties kan het outside IP-adres niet worden meegenomen. Daarnaast gaat bij modificatie de looptijd van het product opnieuw in.

Upgrade mShield naar mShield Redundant

Via CBG Connect kunt u eenvoudig uw mShield dienst upgraden naar de redundante versie. Tevens kunt u hierbij een ander level kiezen. Houdt bij het upgraden rekening met upgradekosten.
Downgraden van een mShield Redundant naar een non-redundant mShield is ook mogelijk. Informeer bij CBG Connect naar de kosten.
Bij modificaties kan het outside IP-adres niet worden meegenomen. Daarnaast gaat bij modificatie de looptijd van het product opnieuw in

6 Technische specificaties

mShield is een complete firewall welke eigenschappen als statefull packet inspection, (advanced) NAT, inkomende en uitgaande rules en de robuustheid van een Cisco Firewall combineert in 1 product. Een aantal aanvullende voordelen van dit product is het feit dat de hardware (en het onderhoud hierop) geregeld worden door RoutIT. Tevens wordt het software onderhoud en de aanvullende contracten met Cisco door RoutIT geregeld en hoeft de klant hiervoor verder niets te doen. Het operationeel beheer (security rules, NAT rules e.d.) wordt geheel door CBG Connect verzorgd en kunnen real-time via de management interface ingegeven worden.
De dienst wordt door RoutIT geleverd en direct aan de backbone (op het Cisco 6500 platform) gekoppeld. Voordeel hiervan is dat de performance van de mShield ongeëvenaard is (~10Gbps) en er tot twee miljoen concurrent sessies opgebouwd worden (125.000 sessies p/s).

Basisinrichting van mShield

Bij de bestelling van mShield zal RoutIT een basisinrichting verzorgen. De basisinstellingen zijn:

- mShield mag beheerd worden vanuit het hele inside netwerk. Beheer vanuit outside staat default uit.
- Echo en echo-reply staan default aan op de inside interface.
- Echo-reply staat default aan op de outside interface.
- Alle inside netwerken worden standaard naar het outside publieke IP adres vertaald van de mShield bij verbindingen naar het internet.
- Default mogen alle inside netwerken naar buiten op basis van IP adres.
- Default staat alles naar binnen dicht.
- Logging is default niet geconfigureerd.
- 2 interfaces (inside (security 100), outside (security 0))

Verantwoordelijkheden CBG Connect

CBG Connect dient RoutIT te voorzien van essentiële informatie voor de te leveren RoutIT mShield. CBG Connect dient de volgende informatie aan te leveren:

- De IP VPN waar mShield aan dient te worden gekoppeld.
- De gebruikersnaam en het wachtwoord waarmee CBG Connect straks zijn mShield gaat beheren.
- Mocht er meer dan één publiek IP adres nodig zijn, dan dient u dit te worden aan te geven.
- Als de mShield vanuit buiten moet kunnen worden beheerd, dan ook graag het beheer IP adres doorgeven.
- Naast het voorzien van essentiële informatie is CBG Connect na oplevering van de mShield verantwoordelijk voor het beheren en inrichten van mShield.

Beheer van de mShield

Het beheren van de mShield firewall wordt door CBG Connect gedaan. De mShield firewall is standaard te bereiken vanuit het inside netwerk door in de browser naar https://172.31.255.254/ te gaan. Hier kunt u inloggen met de gebruikersnaam en wachtwoord welke u heeft doorgegeven aan RoutIT.

7 FAQ mShield

Wie doet het beheer van een mShield?

Het beheer wordt door CBG Connect gedaan.

Hoe kan mShield benaderd worden voor beheer?

mShield kan altijd benaderd worden vanuit de IP-VPN. mShield is in de browser te benaderen via https://172.31.255.254/ . Wanneer mShield vanuit het publieke internet beheerd dient te worden, zal dit in een ticket op de mShield order moeten worden verzocht.

Wat is het publieke IP adres om in een IP-VPN te komen?

Het publieke IP adres van de IP-VPN is op te vragen bij CBG Connect.

Kan het level van een mShield worden gewijzigd?

Ja, dit is mogelijk. Het mShield product kan gemodificeerd worden. Vraag CBG Connect om meer informatie.

8 Algemene kaderzetting van deze dienstbeschrijving

Deze dienstbeschrijving vormt een onlosmakelijk deel van de ondertekende offerte in combinatie met Algemene koop- en leveringsvoorwaarden 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.

Wijzigingen en typefouten voorbehouden.

CBG Connect B.V., november 2016