Dienstbeschrijving
mShield

Een dienst in KPN ÉÉN

Versie : v1.0
Datum : 1 januari 2018

Inhoud

1 Dit is mShield

De mShield dienst van KPN 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 die u geheel zelf kunt instellen. Daarnaast heeft u geen zorgen over updates, performance, licenties en hardware. 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.

1.1 mShield varianten

KPN biedt de volgende mShield varianten:

- mShield (Level 1 t/m 4)
  Voor bedrijven die behoefte hebben aan een uitgebreide firewall voor meerdere verbindingen die in één IP-VPN wolk zitten, biedt KPN 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)
  Hetzelfde als mShield, met als toevoeging dat deze firewall redundant is uitgevoerd.

2 Levels en technische kenmerken

2.1 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.

Hosts, Xlates & Connections

Bij het bepalen van uw keuze voor het mShield level, zijn onder andere het aantal benodigde hosts, xlates en connections belangrijk. Uw partner kan u helpen tot het maken van de juiste keuze.

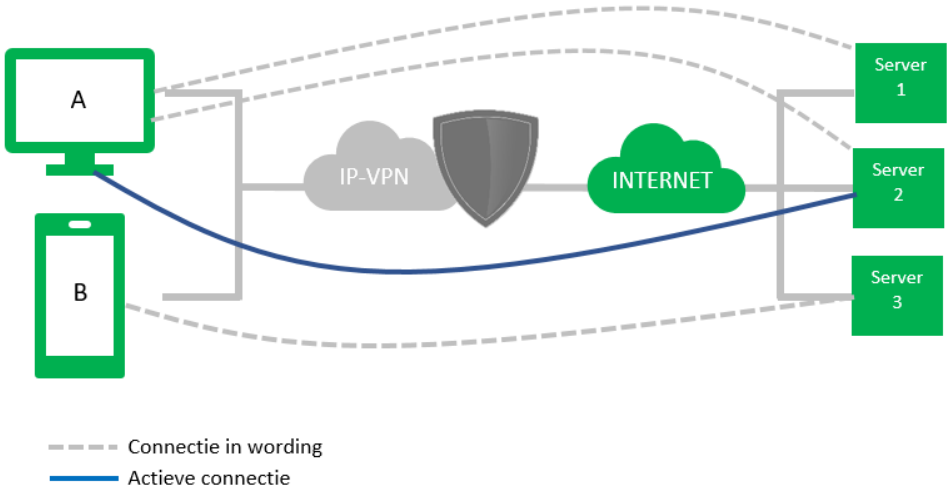
- Hosts
  mShield telt één host per apparaat per connection, wanneer twee apparaten/servers verbinding met elkaar maken. Oftewel, minimaal 2 hosts voor één connection. Een gelijktijdige tweede verbinding tussen dezelfde twee apparaten/servers telt niet mee in de host-telling.

  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. KPN ondersteunt maximaal het opgegeven aantal interfaces per mShield.

2.2 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

3 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 is i.v.m. onderhoud of storing, de secundaire firewall het overneemt.

4 Werking en kwaliteit

4.1 Werking mShield

Door het toepassen van een mShield is het mogelijk een IP-VPN te combineren met een complete firewall. mShield kunt u zelf instellen, of u laat het door uw partner instellen. KPN 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 KPN.

4.2 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 KPN. Hierdoor en door het KPN backbone netwerk, is het mogelijk de dienst aan te bieden met de hoogste kwaliteit zoals u van KPN mag verwachten. Het backbone netwerk van KPN wordt continu gemonitord en waar nodig wordt er (pro)actief gereageerd door KPN. Door deze monitoring kan KPN trends en analyses vergelijken en zodoende zorgen voor voldoende capaciteit.

Het grote verschil van mShield ten opzichte van andere oplossingen is dat er op uw locatie 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 één security policy. Elke locatie behoudt zijn maximale download bandbreedte, omdat de verbinding van de mShield firewall naar het internet maximaal is.

5 Modificaties

5.1 Level modificatie

mShield kent meerdere levels die het aantal resources vertegenwoordigen. U up- en downgraden in resource-level. Er zijn kosten verbonden aan deze aanpassingen, per wijziging.

Bij modificaties kan het outside IP-adres niet worden meegenomen. Daarnaast gaat bij modificatie de looptijd van het product opnieuw in.

5.2 Upgrade mShield naar mShield Redundant

U kunt uw mShield dienst upgraden naar de redundante versie. U kunt ook tegelijkertijd een ander level kiezen. Houdt bij het upgraden rekening met upgradekosten.

Bij een downgrade van een mShield Redundant naar een non-redundant mShield worden downgradekosten in rekening gebracht.

Bij modificaties kan het outside IP-adres niet worden meegenomen. Daarnaast gaat bij modificatie de looptijd van het product opnieuw in.

6 Service Level en levertijd

6.1 Service Level

Bij storingen kunt u contact opnemen met uw partner. De kenmerken van het service level ziet u in onderstaande tabel:

Service Level	Service window	Beschikbaarheidsgarantie	Herstelgarantie
Next business day	Kantoortijden	99,60%	< 8 uur

6.2 Levertijd

mShield producten kennen een levertijd van ongeveer 2 werkdagen.

7 Bijlage: 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 zijn het feit dat de hardware (en het onderhoud hierop) geregeld worden door KPN. Tevens worden het software onderhoud en de contracten met Cisco door KPN geregeld en hoeft u hiervoor verder niets te doen. Het operationeel beheer (security rules, NAT rules e.d.) wordt geheel door uzelf of door uw partner verzorgd en kan real-time via de management interface ingegeven worden.

De dienst wordt door KPN 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 KPN een basisinrichting verzorgen. De basisinstellingen zijn:

- mShield mag beheerd worden vanuit het hele inside netwerk (RFC 1918). Beheer vanuit outside staat default uit, tenzij bij aanvraag een beheer IP-adres opgegeven wordt.
- Echo en echo-reply staan default aan op de inside interface.
- Echo-reply staat default aan op de outside interface.
- Alle inside netwerken (RFC 1918) worden standaard naar het outside publieke IP adres vertaald van de mShield bij verbindingen naar het internet.
- Default mogen alle inside netwerken (RFC 1918) naar buiten op basis de volgende protocollen
- ICMP (echo en traceroute)
- HTTP
- HTTPS
- DNS naar de KPN DNS Resolvers
- NTP naar de KPN NTP Server
- SMTP naar het KPN Mailcluster
- Default staat alles naar binnen dicht, behalve echo-reply en time-exceeded.
- Logging is default niet geconfigureerd.
- 2 interfaces (inside *security 100*, outside *security 0*)