

# Ouderlijk toezicht

Hans Sodaar

**Kinderen komen makkelijk op plekken op het internet waar je ze liever, afhankelijk van hun leeftijd, (nog) niet wilt zien ronddolen. Er bestaan een aantal middelen die hun wel vrijheid geven, maar zonder dat je je zorgen hoeft te maken. Hieronder wordt toegelicht hoe je op twee manieren de internettoegang kunt beheersen.**

In aansluiting op het artikel 'Veiligheid, who cares?' van Ernst Roelofs in de vorige SoftwareBus, wil dit artikel ingaan op de controle op het internetgebruik van kinderen. Afhankelijk van hun leeftijd en ontwikkeling zou je de toegang tot sommige typen sites willen afschermen. Het beperken heeft echter een aantal facetten. De eerste is de sociale kant, richting het kind. Het advies van deskundigen op dit gebied is om er open over te zijn en het bespreekbaar te houden. Het tweede is: 'Hoe regel ik het technisch en hoe heb ik inzicht in het nakomen van de gemaakte afspraken?' Over dat laatste gaat dit artikel.

## Voor welke systemen is dit toepasbaar?

Met de pc's, smartphones en tablets en hun diverse operating systemen zijn er vele mogelijkheden om het internet te verkennen. Bovendien is er legio keus uit browsers. Voor het selectief filteren van sites bestaan meerdere commerciële en freeware oplossingen. Voor dit artikel is gekozen voor twee gratis oplossingen, nl.: 'OpenDNS' van OpenDNS en 'K9 web-protection' van Blue Coat. Deze zijn beide toepasbaar voor Windows, MacOS, iOS en Android. Voor Linux is alleen OpenDNS toepasbaar. Gekeken wordt naar het gebruik in een (eigen) bekabeld of draadloos netwerk en in een publieke omgeving.

## OpenDNS



Hoe werkt het?

OpenDNS is een dienst die aangeboden wordt door gebruik te maken van de OpenDNS-servers; deze staan o.a. in Amsterdam, Frankfurt en Londen. Deze zorgen dan voor je DNS-lookup. Het ondersteunt netwerken met statistische en dynamische IP-adressen. De op je netwerk ingestelde DNS-serveradressen moeten vervangen worden door de DNS-serveradressen van OpenDNS t.w. 208.67.222.222 en 208.67.220.220. De bescherming werkt op basis van je IP-adres. Hiervoor moet je een account aanmaken bij OpenDNS en filters instellen. Voor netwerken met een dynamisch IP-adres is er een IP-updater (Windows en MacOS) die in de gaten houdt of je IP-adres verandert en die ervoor zorgt dat de relatie tussen je instellingen en je IP-adres in stand blijft.

## Installatie

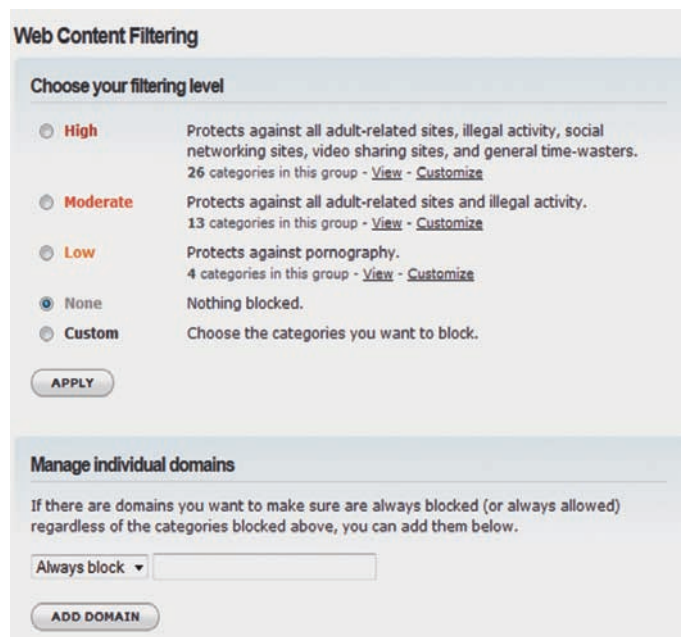
Het installeren is afhankelijk van de netwerktopologie. Er zijn drie mogelijkheden:

1. Bekabeld netwerk: door de DNS-serveradressen in de router of het modem aan te passen.
2. Individuele pc's: via de netwerk DNS-instellingen op de pc.
3. Wi-Fi-netwerk: door de DNS-instellingen op de Wi-Fi-router of de netwerk router aan te passen. Op smartphones en tablets zijn er dus géén speciale filter-mogelijkheden anders dan die voor een eigen Wi-Fi-netwerk. Uitgebreide instructies voor alle drie de toepassingen staan op de site.

## Filtermogelijkheden

Er wordt een keuze geboden uit een aantal standaardinstellingen, maar deze zijn wel aanpasbaar aan de eigen wensen. De standaardinstellingen zijn:

- Hoog: beschermt tegen alle aan volwassenen gerelateerde sites, illegale activiteiten, sociale netwerken, video sharing-sites, etc., onderverdeeld in 26 categorieën.
- Matig: beschermt tegen alle aan volwassenen gerelateerde sites, illegale activiteiten, onderverdeeld in 13 categorieën.
- Laag: beschermt tegen pornografie, onderverdeeld in 4 categorieën.
- Geen: geen filtering.
- Aangepast: eigen keuze van de te filteren websites.
- White List en Black List: filtering op zelf te bepalen websites.



Figuur 1: OpenDNS filterniveaus

## Rapporten

Via het dashboard van je account kunnen de statistieken gedefinieerd worden en kan gekeken worden naar de logs van de bezochte sites voor je opgegeven netwerken. Als extra is er ook een mogelijkheid om de zoekresultaten voor plaatjes te beperken voor diverse browsers.

Een minpunt is, dat het niet werkt op mobiele apparaten buiten het eigen netwerk.

## K9 webprotection



Hoe werkt het?

De webfiltering van K9 werkt niet op basis van het IP-adres, maar maakt gebruik van een lokale database voor de filtering op de pc; bij mobiele apparaten, als smartphones en tablets, wordt gebruik gemaakt van de K9 webbrowser met een standaardinstelling. Hierbij speelt dus een veranderend IP-adres geen enkele rol. De filtermogelijkheden voor pc en mobiele apparaten zijn wel verschillend.

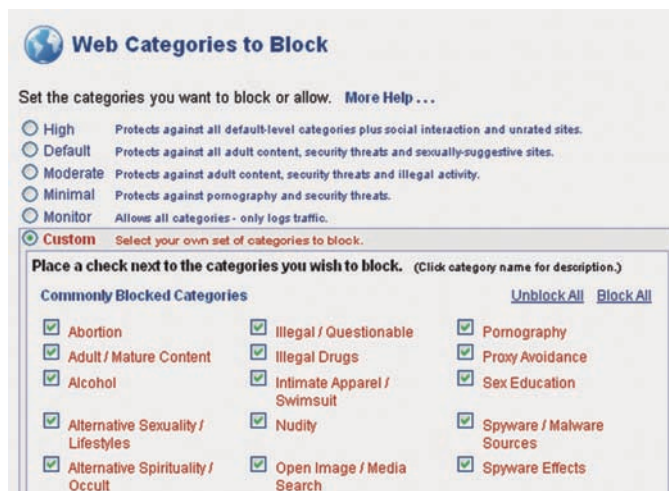
## Installatie op de pc

Ga naar de K9 website, vul de gegevens in en volg de aanwijzingen. Download en installeer de software en ga aan de slag met de instellingen. De instellingen en de rapportages zijn beschermd met een wachtwoord tegen aanpassingen en deïnstallatie.

## Filtermogelijkheden

De software heeft de volgende features:

- instellen van toegang tot meer dan 70 typen websites;
- forceren van 'safe search' of blokkeren van 'unsafe search';
- zetten van tijdrestricties voor webtoegang;
- 'black list' en 'white list' voor zelf te bepalen sites;
- toegang tot geblokkeerde sites door middel van het administratorwachtwoord.

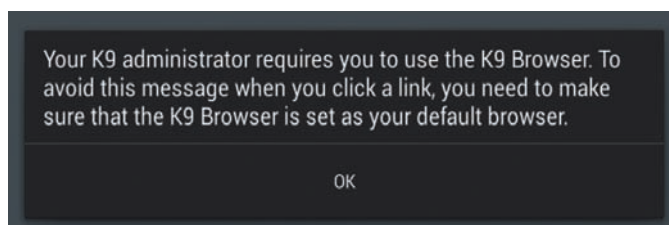


Figuur 2: Voorbeeld blokkeringscategorien

## Installatie op mobiele apparaten

Hierbij wordt gebruik gemaakt van de K9 webprotection browser die als app beschikbaar is in de iTunes en de Google Play store. Alle instellingen op het apparaat worden beveiligd met een wachtwoord voor de administrator.

Het gebruik van de al aanwezige apps op het toestel kan beheerd worden, net zoals het (de)installeren hiervan.



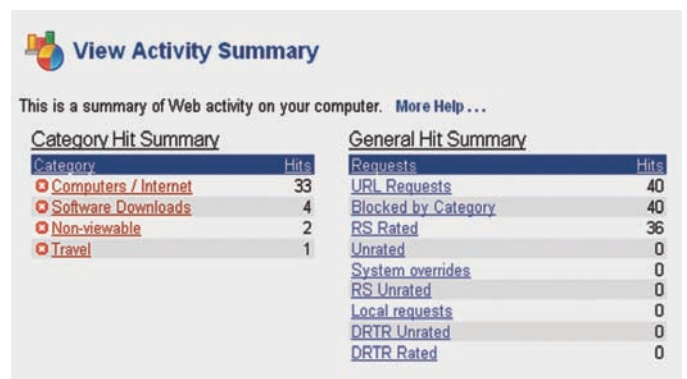
Figuur 3: Blokkeringsmelding Android

De K9-browser is gebaseerd op Firefox. De app blokkeert alle aanwezige andere browsers (zie figuur3). Deze mogelijkheden en instellingen wijken iets van elkaar af in de iOS- en Android-versies, maar worden goed gedocumenteerd op de site.

De volgende typen sites worden door de browser gefilterd:

- inhoud voor volwassenen en offensieve inhoud: Pornografie, geweld ...
- potentieel gevaarlijke inhoud: Phishing, spyware ...
- potentieel illegale inhoud: Peer2peer, gokken ...
- controversiële ouder-kind topics: Abortus, dating ...

Het betreft een standaardinstelling die niet individueel aan te passen is, zoals met de pc-versie van K9.



Figuur 4: Activiteitenrapportage

## Rapporten

Uitgebreide rapportages kunnen worden bekeken van de internet activiteiten, gesorteerd op diverse zelf te kiezen criteria.

## Conclusie

De keuze uit de twee hier genoemde opties zal bepaald worden door de eigen wensen en de situatie ter plekke.

Bij de één worden de filtergegevens centraal opgeslagen op een server in de cloud, bij de ander staan de instellingen op de locale pc. Wat betreft filtering voor smartphones en tablets is maar één van de twee te gebruiken. Beide zijn voor particulier gebruik gratis.



Vergeet vooral niet er met je kind over van gedachten te wisselen.

Enkele links:

<https://www.opendns.com/home-solutions/>  
<http://www1.k9webprotection.com/>  
<http://www1.k9webprotection.com/getk9/documentation>