GreeNet's Parental Control Solution Briefing

Table of Contents

Overview

Parental Controls are functions that enable parents to limit and control their children's access to the internet. Ideally, a parental control system will allow a parent to customize a child's internet experience regardless of location or connection type. Whether they are accessing the web from home internet or the children's smart devices using mobile data services, the rules will be implemented. The reasons to control access to the internet for children are many, but common reasons are; some content may be deemed unsuitable for the under-aged, maturity level, adultery, religious beliefs, violence, illegal and sensitive information, and more. Typical functions of parental control systems include:

1. Content filtering – user-specified filtering of URL's, Applications, etc
2. Usage controls – time of the date and number of hours to use
3. Monitoring and tracking – regular reports showing usage details, including attempts to access restricted content sent to the service subscriber
4. Device controls – white-list or black-list devices registered under the subscription

Many vendors offer client software to be installed on the phone or device to enable parental control functions. This legacy approach of client-based controls per device quickly becomes unmanageable if a parent has multiple devices to manage. The software also slows down the device and quickly drains the battery. Children are also often able to find ways to disable and bypass the controlling software. As a result of these limitations, device based parental controls are not sufficient and are therefore no longer popular.

Research from Ofcom (http://www.ofcom.org.uk) shows that between 40-50% of parents with children under 15 years of age have installed parental control solutions to protect their children. This demand has driven vendors to develop new solutions to overcome the limitations of legacy products. The new generation of solutions are "network-based", require no software on the device, are subscriber provisioned, and offer the highest administration

right for all the devices registered under the subscription. The devices are protected, whether connected to home WIFI, public WIFI, or on the move with mobile data. Communication Service Providers, whether they provide fixed, mobile, or other access services, now have the advantage of being able to offer network-based content controlling solutions, which is in general called *network-based parental control solutions* as a value-added service to their customers.

There are many good reasons why parents want to restrict internet access and content viewing for their children. It could be from a desire to limit the number of hours of use per day, confining the time of the day of use, restricting pornography and any other inappropriate content, controlling access to online gaming, removing the capability for online shopping, and many more. Parents who are using network-based parental controls know that their children are protected from unwanted content. The parents who subscriber see value in the solution and are happy to spend extra subscription fees for this service. As a result, the CSPs can generate additional revenue and increase APRU.

Market Dynamic and Opportunity

There are many parental control solutions available in the market. Some are installed in each device; some are installed in the home router, and only a few are implemented in the CSP network. None of the device or home router-based solutions are sufficient as a parental control solution, as children today quickly learn technology often much better than some parents; they often find ways to manipulate device settings and home router settings to bypass the restriction. Therefore, some telecom authorities request their CSPs to implement network-based-parental control solutions as part of the safeguard and clean network motivation to protect the juniors.

Network-based parental control is more than URL filtering; it also gives the functions of allowing only some apps, such as Facebook, WhatsApp, or online gaming in free time, but

blocking during homework time, sleeping time, and family time. The solution comes with a self-management portal giving the subscription owner the full right to register and manage all devices, even though family members use them at home with the internet or on the move with mobile data.

With the self-support portal, the CSP can minimize the operating costs while giving full control to the subscriber owner to change the setting at their desire.

GreeNet's Parental Control Solution and Capability

GreeNet's Parental Control Solution runs on GreeNet's iNAS Architecture and is implemented in the communication service provider's network. It provides the CSP a set of dynamic and real-time management tools to link between the CSP's subscriber database used for portal provisioning and subscriber's registered devices. GreeNet's solution provides the following functions:

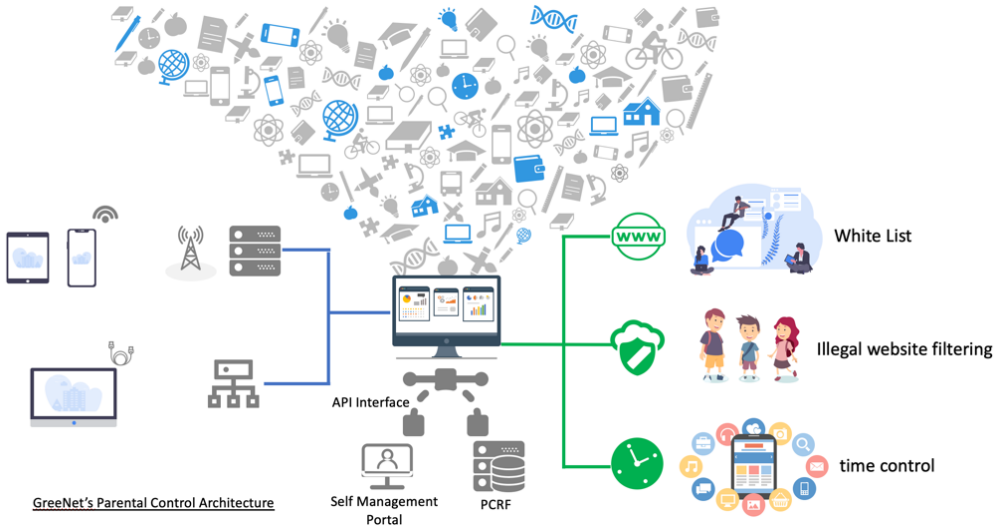
- Real-time content management and filtering
- White-and-Black-List filtering
    - it is a database with millions of URLs and Apps that are categorized as white-list or black-list for filtering use. The database is updated regularly to keep up with the latest list. For example, URL and App for pornography, child pornography, gambling, gaming, social network services, hatred contents, and sensitive contents.
- User Specified White and Black List
    - The subscriber can create his list to use for each registered device
- User behavior and statistical analytics

- The subscriber can review usage statistics for each registered device, such as time spent on specific apps and the number of hours spent on web browsing, attempts to access restricted applications or websites.

- Service provisioning
  - Service Portal
    - User Registration and Un-registration
  - Self-management portal
    - User Profile Management: Add, Delete or modify device. Devices are identified by name; such as John's iPhone
    - Content Profile Management: Block and unlock contents

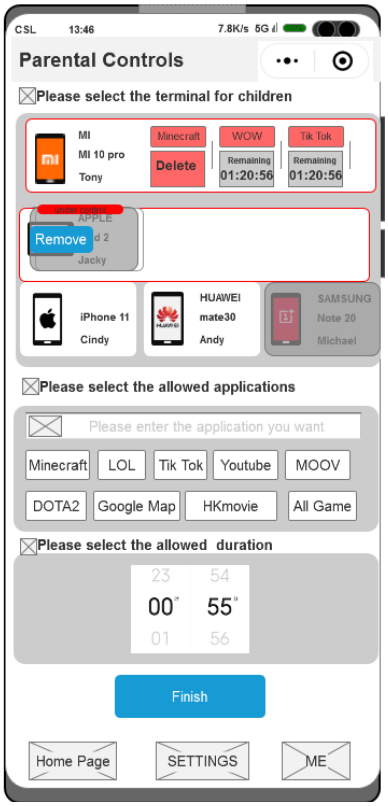
High-Level Solution Architecture

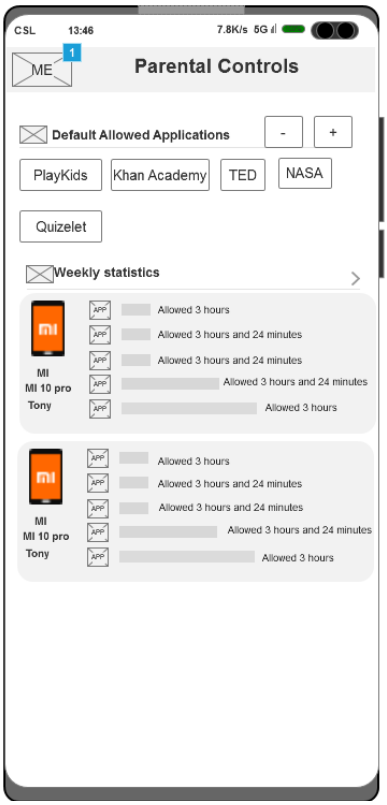
The key components of the GreeNet's Parental Control Solutions are described in the diagram below.



Self-Management Portal Screen Shots

The self-management portal app runs on a subscriber's device in a web browser; it is not an application and does not require anything to be installed. The portal provides the capability for registering new devices to monitor, application white-or-black-list, time day use, and access to reports.





About GreeNet

GreeNet provides intelligent network service awareness solutions for enhancing customer satisfaction and monetization services for CSP customers. The company specializes in network service awareness, data and control plane analytics, and regulatory compliance's security

solutions. Founded in 2003, GreeNet has 300 experienced in-house developers dedicated to developing innovative services and security solutions to meet market demands.

GreeNet has more than 250 deployments in 160 cities globally. The total bandwidth capacity installed by our customers is more than 400 Terabytes for various applications.

GreeNet's intelligent iNAS solution is developed with the industry's most advanced software-based DPI technologies. The solutions are used in the fixed, mobile, IoT, and any network access environment. It provides end-to-end IP network visibility, data analytics, network filtering, and network security solutions, including anti-Fraud, anti-Malware, DDoS Mitigation, and Parental Control.

For details, please visit www.greenet.co, contact one of our sales locations or email us at sales@greenet.co.