Contents

Parental Control Goals

The goals of parental control described herein below are as following:

- no internet access for children devices at night time
- no access to adult-only sites for children devices all the time

In general, every device on network is restricted except the well-known parental devices. It means that every household guest is restricted by default, e.g. when a child's friend comes to visit, they are restricted as well.

Remember that this tutorial protects your children at your home only. Another part of parental control is to disable mobile internet on the children's phones by your telecommunication operator. And don't forget the most important part of parental control - talk to your kids about the danger they can face on internet.

Separate Parental and Children Devices

To achieve parental control's goals we need to separate devices connected to network into two groups.

Parental Devices

In order to earmark parental devices we have to know their MAC addresses. If you don't know where to get these strange numbers, let's google out for a phrase *how to find mac address*.

Let's assume we have the following devices on the network:

Device	MAC Address
Mom's phone	12:34:56:ab:cd:ef

Dad's phone	12:34:56:78:ab:cd
Dad's notebook	12:34:56:78:90:ab
Son's tablet	aa:bb:cc:12:34:56
Daughter's phone	aa:bb:cc:dd:12:34
Children notebook	aa:bb:cc:dd:ee:12

Looking at the table we can see that first three devices belong to parents.

We assign a device to parental devices group by assigning static IP address from parental IP address range to the device. For purpose of this tutorial any device which has IP address from range **192.168.1.2 - 192.168.1.99** is considered as parental. In our case we assign static lease as following:

MAC Address	IP Address
12:34:56:ab:cd:ef	192.168.1.2
12:34:56:78:ab:cd	192.168.1.3
12:34:56:78:90:ab	192.168.1.4

See Static DHCP Configuration to learn how to do it.

Note that some mobile devices with Android 5.1 Lollipop (e.g. VK 700x with firmware from end of 2015) and devices with newer iOS have "dynamic" MAC address which is changing after each Wi-Fi on/off or after each device restart. Such a device cannot be managed and always falls into the set of restricted devices.

Children Devices

Any device which is not listed in static IP address assignment is considered as children one. A device with no static lease obtains IP address from DHCP configured range. In our case we set the dynamic lease as following:

- Start IP address: **192.168.1.100**
- Maximum DHCP Users: **50**

This give us the IP address range **192.168.1.100 - 192.168.1.149** which we apply restrictions on.

See DHCP Server Configuration to learn how to do it.

No Internet Access for Children at Night

First goal of the parental control is cut out the children from internet at night time. In our case we want to deny internet access from 10pm to 6am. Due to policy' setup limitations we have to create 2 almost identical access policies as following:

Policy	1	2
Status	Enable	Enable
Policy Name	No Internet Night	No Internet Morning
List of Clients	192.168.1.100 - 192.168.1.149	192.168.1.100 - 192.168.1.149

(IP Address Range)		
Deny / Filter	Deny	Deny
Days	Everyday	Everyday
Times	From 22:00 To 23:59	From 0:00 To 5:59

See Denying Internet Access to learn how to do it.

No Access to Adult-Only Sites For Children

Second goal of parental control is to prevent children viewing websites with adult-only content like dating, nudity, pornography and/or drugs and weapons. The degree of prevention is up to your decision as you can see below. We need to integrate several services and settings to restrict the children from unwanted content.

OpenDNS (+ DNS-O-Matic)

Let all the dirty work with evaluating which site is or is not appropriate for children for OpenDNS. If you have dynamic public IP address you have to configure also DNS-O-Matic service.

See OpenDNS Basic Setup and OpenDNS with Dynamic IP to learn how to do it. Do not follow the instructions about DNS Interception, we solve it in more user friendly way.

DNS Interception on Children Devices

In order to prevent children to bypass OpenDNS server we prohibit DNS requests for children IP address range by filtering DNS service as following:

Policy	3
Status	Enable
Policy Name	DNS Interception
List of Clients	
	192.168.1.100 - 192.168.1.149
(IP Address Range)	
Deny / Filter	Filter
Days	Everyday
Times	24 Hours
Blocked services	dns

DNS Override on Parental Devices

Since we have DNS interception active only on children devices we can setup non-filtering DNS servers on parental devices. If you do that, you also loose phishing protection provided by OpenDNS on parental devices. If you choose to have totally free internet just google out for *how to set dns in windows* or use the following command on Windows machines to set Google public DNS servers:

```
netsh interface ip add dns name="your_network_connection_name+here" addr=8.8.8.8 index=1
```

```
netsh interface ip add dns name="your_network_connection_name+here" addr=8.8.4.4 index=2
```

Consider to use a geographically near DNS server (ideally placed in your country) to minimize latency.

Conclusion

Note that no protection in digital world is 100% working. There are dozens of tutorials how to avoid any restriction and depends only on your children's technical skills and time available to overcome one. Again, the most important thing in your children's internet security is to talk to them about the threats.

If you have setup parental control you can consider also other pleasant setting on your home network such as Ad blocking, Printer Sharing or choose the one from dozen of DD-WRT tutorials.