

# Firewall Profiles

## Introduction

- Firewall Profiles are the most advanced tool available in MESHdesk and APdesk to manage usage.
- It allows you to tailor make a Firewall Profile and assign it to an Exit Point or selected user devices.
- As an overview of available tools to manage usage we have:
  - **WiFi Schedules** → Turns a specific SSID on and off on selected times.
  - **Throttling and Blocking Users** → These are on selected user devices and always applied.
  - **Firewall Profiles** → Swiss Knife that allows you to roll your own.
- The rest of this document will cover Firewall Profiles in detail.

## Design Philosophy

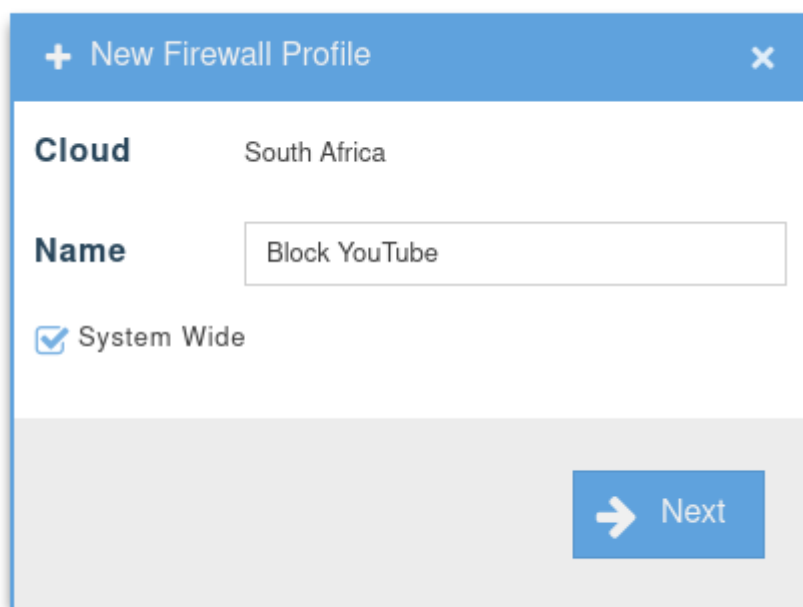
- The design philosophy followed by most components in RADIUSdesk is one of *define once, apply to many*.
- With the Firewall Profiles we also follow this philosophy.
- A Firewall Profile can be applied to user devices that connects to the MESHdesk and APdesk networks.
- A Firewall Profile can also be applied to an Exit Point which is defined on a MESHdesk and APdesk network, e.g. a bridge, a NAT/DHCP gateway or a Captive Portal.
- We also allow the root user to define site wide Firewall Profiles.
- Site wide Firewall Profiles are available to **all** clouds.
- This further reduces duplication.

## Creating A Firewall Profile

- The Firewall Profile Applet is available under **Other → Firewall**
- A Firewall Profile consists of the following:
  - Firewall Profile Name
  - One or more Rules
  - A Rule in turn can contain one or more Apps (If the Rule's category is selected as **App**)
- Lets create a simple Firewall Profile that will block YouTube between 7AM and 5PM during weekdays.

## Blocking YouTube During Week Days

- Click on the Add Toolbar Button to create a new Firewall Profile



**+ New Firewall Profile**

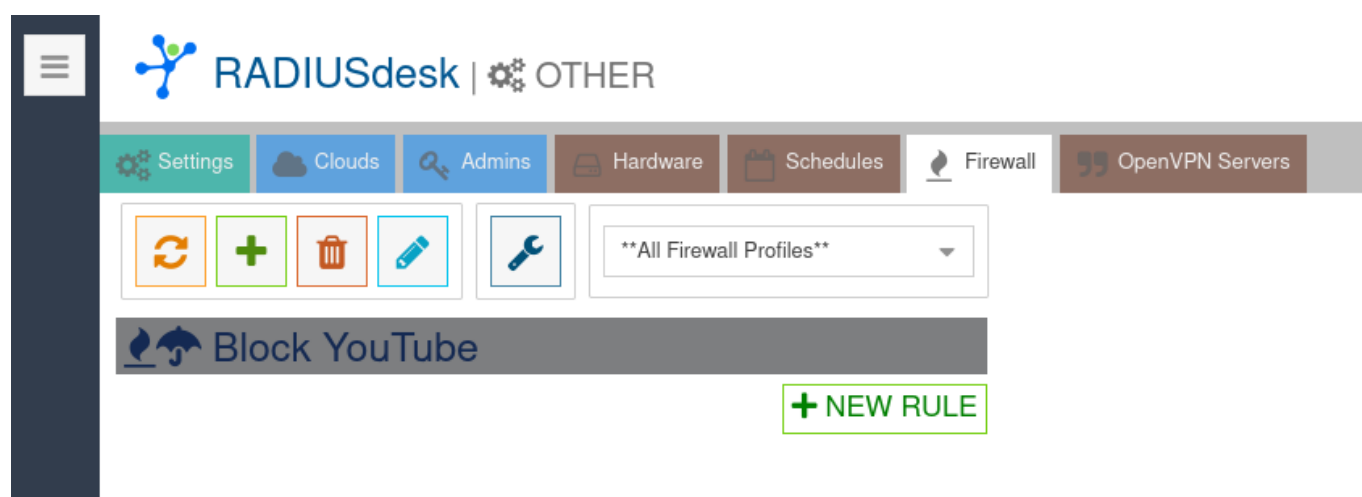
**Cloud** South Africa

**Name** Block YouTube

☒ System Wide

**Next**

- We selected to make it system wide (Indicated by the Umbrella Icon in the Name banner.)



- Next we can start to add Rules.
- If a rule's Category is App you should select one or more predefined Firewall Apps to be part of the rule.
- An App has to be defined and contains a list of IP Addresses. (For the technical minded, these will be bundled into a **set** to be used by **nftables**.)

## Creating The YouTube Firewall App

- To manage Firewall Apps, click on the toolbar button with the wrench (Tool-tip Firewall Apps)
- This will open a new tab with a list of Firewall Apps.

The screenshot shows the RADIUSdesk web interface. The top navigation bar includes 'Settings', 'Clouds', 'Admins', 'Hardware', 'Schedules', 'Firewall', 'OpenVPN Servers', and 'Firewall Apps'. The 'Firewall Apps' tab is active. Below the navigation bar, there is a toolbar with icons for refresh, add, delete, and edit. A list of firewall apps is displayed, with 'YouTube' selected. The 'Edit Firewall App' dialog box is open, showing the following fields:

- Name:** YouTube
- FA Code:** &#xf167;
- Elements:** 172.217.0.0/16
- Comment:** Block YouTube
- ☒ System Wide

The dialog box has an 'OK' button at the bottom right.

- Two items that need more explanation.
  - **FA Code.** This is the Font Awesome code which will be translated to an easy to recognize Icon / Glyph.
  - Although it is cosmetic, it is also functional to identify Apps that's part of a rule.
  - You can consult this URL for available Icons: <https://fontawesome.com/v4/cheatsheet/>
  - **Elements.** These are IP addresses or ranges which will be used by nftables as part of their sets.
  - You can consult this URL to read up more on Sets and Elements inside Sets: <https://wiki.nftables.org/wiki-nftables/index.php/Sets>
- Now we can return to our Firewall Profile to complete the new rule.

## Rule for YouTube

- The Add and Edit Rule form is very easy to use and also to make changes to existing rules.

The screenshot shows the RADIUSdesk interface with the 'Firewall' tab selected. The main panel displays a 'Block YouTube' rule under 'Block every week' with a schedule from 7:00 to 17:00. A '+ NEW RULE' button is visible. An 'Edit Firewall Profile Entry For' dialog is open, showing settings for blocking YouTube every week from 7:00 to 17:00.

- You can combine as many rules as you like in one Firewall Profile.
- Here we keep it simple by just blocking YouTube.

## Using The Firewall Profile

- Next we can associate it with an Exit Point on a MESH network or an AP Profile.

The screenshot shows the RADIUSdesk interface with the 'Meshes' tab selected. The 'Edit mesh exit point' dialog is open for 'Henley 01', showing settings for 'Connects with' (Sub-Eynsham-909) and 'Apply Firewall Profile' (Block YouTube). The background shows the 'Meshes' tab with a table listing exit points.

Type	Exit points	Firewall Profile
Bridge	Henley 01	Block YouTube

- Alternatively you can associate it with a client's device.

The screenshot shows the 'Apply Firewall Profile' dialog box on the left and the 'Top 10 Devices' table on the right.

**Apply Firewall Profile Dialog:**

- Scope: ☒ Cloud Wide, ☐ Mesh Only
- Firewall Profile: Block YouTube
- ☐ Remove Firewall
- SAVE button

**Top 10 Devices Table:**

Alias / MAC Address	Data Total
Linux-01	240.0 Mb
Linux-02	4.9 Mb
Dirk-Phone	3.5 Mb
Koos-Phone	2.0 Mb

## Technical Details

- If you are an old hand with Linux you are probably very familiar with **iptables**.
- In the old days firewalls were done using **iptables** and in case you needed to do packet management on layer two you would use **ebtables**.
- Fast forward to today and we have the much more advanced and user friendly **nftables**.
- nftables allows you to do packet management on layer three and layer two.
- OpenWrt version 22.03 migrated to use nftables instead of iptables.
- This means that the feature will require OpenWrt version 22.03 or higher based firmware to work correct.
- We took the opportunity to take advantage of this improvement and are using this with the Firewall Profile.

## Using Available Meta Data

- With nftables one can create filters based on *meta data*.
- Meta data is data that is available but which are **not part of the traffic** flowing between two hosts on the Internet.
- This includes detail about the hardware (e.g. the interface through which the traffic flows)
- It also includes detail about the time when the traffic is flowing.
- With these meta data filters that is available we formulated the options that you can select when adding a rule to a Firewall Profile.
- One aspect which makes our implementation unique is the fact that we work on layer two and not layer three.
- The reason for this is that MESHdesk and APdesk allows you to create bridged networks where the IP Address management (DHCP) can be done by another device on the network.
- By working on layer two it allows us to formulate rules without the requirement to know the IP Address of a device or Exit Point to which the Firewall Profile is associated with.
- You will need the compulsory **kmod-nft-bridge** nftable module.
- Make sure it is included with the OpenWrt based firmware.
- The **adv\_meshdesk** bridge table is where things are happening.
- You can inspect the table using the following command **nft -e -a list table bridge adv\_meshdesk**.

```
nft -e -a list table bridge adv_meshdesk
```

```

table bridge adv_meshdesk { # handle 2
    set YouTube { # handle 4
        type ipv4_addr
        flags interval
        elements = { 172.217.0.0/16 comment "Block YouTube" }
    }

    set md_lan { # handle 5
        type ipv4_addr
        flags interval
        elements = { 10.0.0.0/8, 172.16.0.0/12,
                    192.168.0.0/16 comment "Private IP Addr LAN" }
    }

    set md_internet_not { # handle 6
        type ipv4_addr
        flags interval
        elements = { 10.0.0.0/8, 172.16.0.0/12,
                    192.168.0.0/16 comment "Private IP Addr Excl
For Internet" }
    }

    chain forward { # handle 1
        type filter hook forward priority 0; policy accept;
        meta day { "Monday", "Tuesday", "Wednesday", "Thursday",
"Friday" } meta hour "07:00"- "17:00" iif "zero0" ip daddr @YouTube counter
packets 0 bytes 0 drop comment "DROP ON zero0," # handle 8
    }

    chain input { # handle 2
        type filter hook input priority 0; policy accept;
        meta day { "Monday", "Tuesday", "Wednesday", "Thursday",
"Friday" } meta hour "07:00"- "17:00" iif { "one0", "two1" } ip daddr
@YouTube counter packets 0 bytes 0 drop comment "DROP ON two1,one0," #
handle 11
    }

    chain output { # handle 3
        type filter hook output priority 0; policy accept;
    }
}

```

- Here you can see the rules which were generated for the Youtube Block Firewall Profile which we defined and applied on a NAT/DHCP and also a bridged exit point.
- The forward chain rule is for the bridged exit point.
- The input chain rule is for the NAT/DHCP exit point.
- As you can see our time of day and also the days to apply is in the meta day and meta hour parts respectively.

From:

<http://www.radiusdesk.com/wiki/> - **RADIUSdesk**

Permanent link:

<http://www.radiusdesk.com/wiki/meshdesk/nft-adv-block>

Last update: **2023/05/11 07:17**

