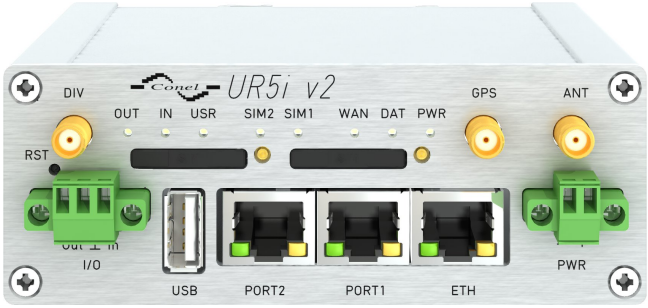
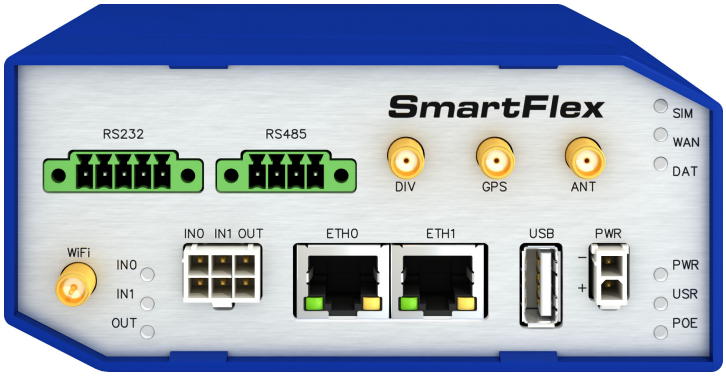
User Module

URL Blocker

APPLICATION NOTE





ADVANTECH

Used symbols

Danger – Information regarding user safety or potential damage to the router.

Attention – Problems that may arise in specific situations.

Information or notice – Useful tips or information of special interest.

Example – example of function, command or script.

Advantech B+B SmartWorx s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. APP-0016-EN, revised on November 30, 2018. Released in the Czech Republic.

Contents

1 User Module Description 1

2 Configuration of URL Blocker 2

3 Recommended Literature 5

List of Figures

1 Router with *URL Blocker* user module installed 1
2 *URL Blocker* menu 1
3 Disabled URL blocking 2
4 Example of blocking enabled 2
5 Enabled URL blocking 3
6 Example of redirecting mode 3
7 Default information page after redirection 4
8 Upload custom welcome/banned page form 4
9 Successful upload of custom welcome/banned page 4

1. User Module Description

URL Blocker user module enables blocking of certain domain names (URLs) so the users connected to the Advantech router cannot access them. Blocking is based on iptables rules (*Blocking* mode) or intentionally forged DNS records sent from Advantech router to connected users (*Redirecting* mode). There are 16 fields in configuration form so it is possible to block up to 16 different domains with the *URL Blocker* user module. Note that blocking does not work when the traffic is in encrypted tunnel (domain name cannot be read from packets).

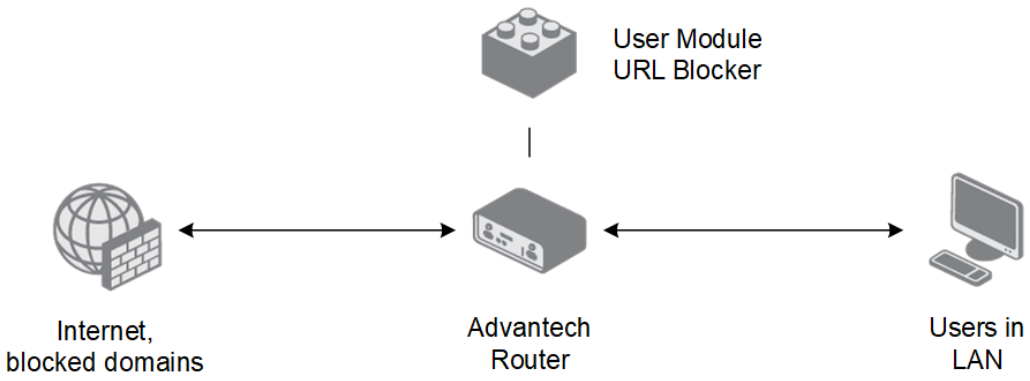


Figure 1: Router with *URL Blocker* user module installed

The *URL Blocker* user module is not part of the router's firmware. It can be downloaded from https://ep.advantech-bb.cz/user-modules. The installation process for the user modules is described in the Configuration Manual (see [1, 2, 3 or 4]). The user module is compatible with v2 and v3 routers.

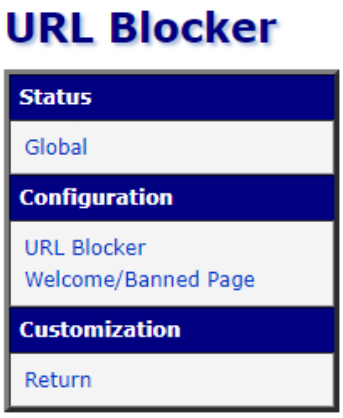


Figure 2: *URL Blocker* menu

The Web interface of the user module is accessible by clicking on the user module's name on the *User Modules* page in the router. On the left there is user module's menu as in Figure 2. There is *Global* landing page in the *Status* section. In the *Configuration* section there is *URL Blocker* page with configuration followed by *Welcome/Banned Page* where custom destination page for redirect mode can be uploaded. You can return to the Web interface of the router using *Return* button in the *Customization* section.

2. Configuration of URL Blocker

After installation, the *Global* page in *Status* section shows this information:

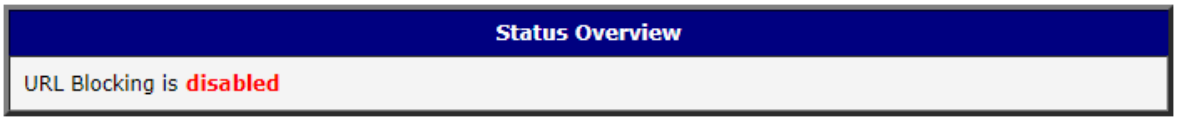


Figure 3: Disabled URL blocking

To enable blocking, go to *URL Blocker* page in *Configuration* section and check the *Enable URL Blocking* checkbox. Two modes of behaviour are possible: 1) **Blocking**, where the blocked page shows just browser DNS error, or 2) **Redirecting**, where the custom blocked page information is shown to the user. Choose *Blocking* option in the select field, fill in the intended domains you want to block and click the *Apply* button.

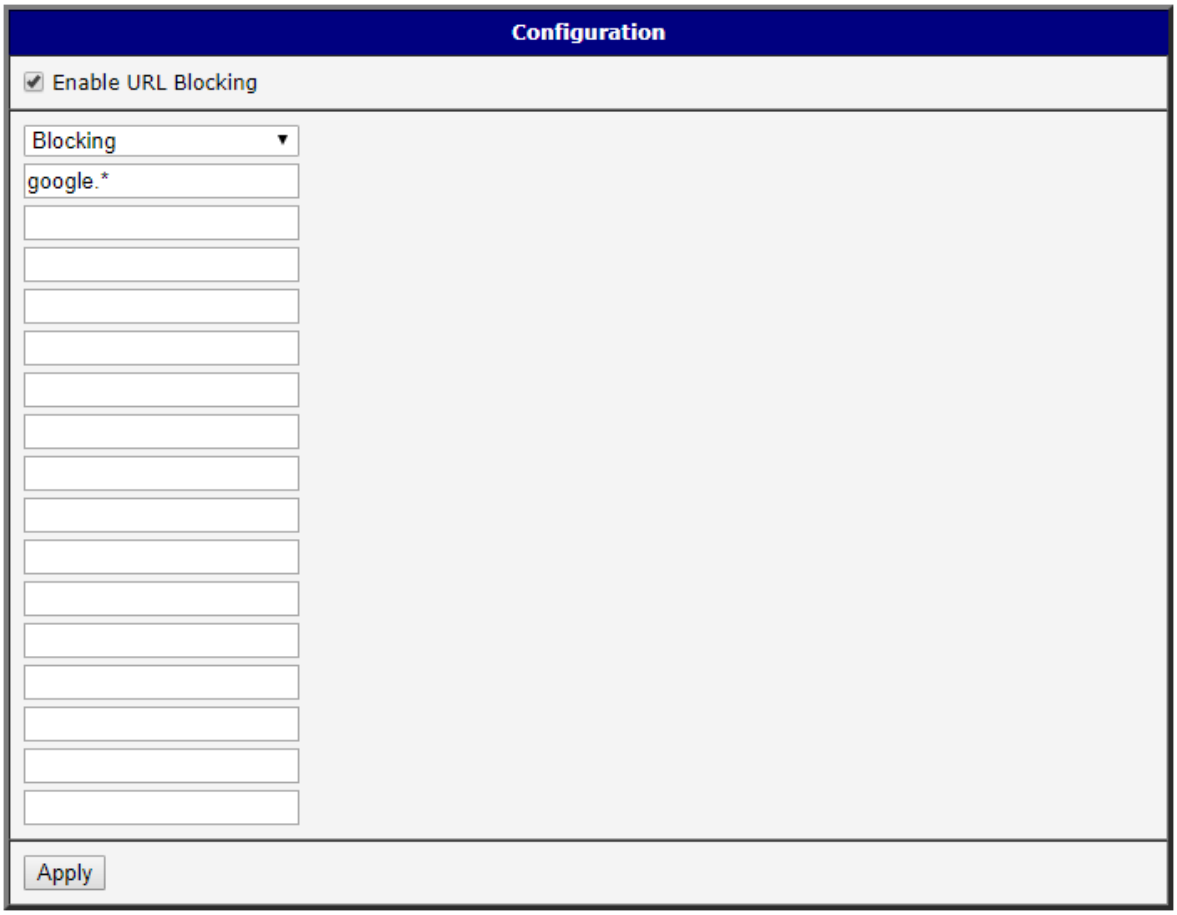


Figure 4: Example of blocking enabled

Now there is enabled information showing on the *Global* page in the *Status* section:

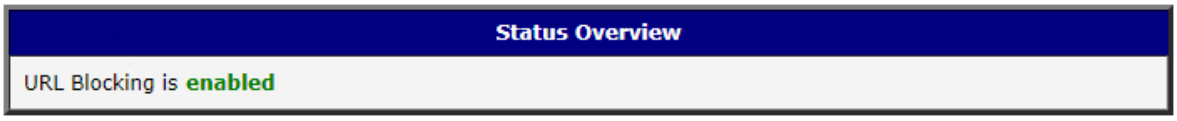


Figure 5: Enabled URL blocking

In *Blocking* mode you can use asterisk * character as a substitute for top level domain. You can see this in Figure 4. All top level domains with the same domain name are then blocked. The substitute * character does not work in the *Redirecting* mode. The redirection works in HTTP only. In HTTPS, the blocking is used instead (Welcome/Banned page does not appear). All subdomains (www., mail., etc.) of the listed domains are blocked by default in both modes.

Note: when testing the user module configuration, do not forget to clear cache of the browser or restart it. Most of Web browsers cache DNS records for themselves.

There is an example of *Redirecting* mode in the next Figure.

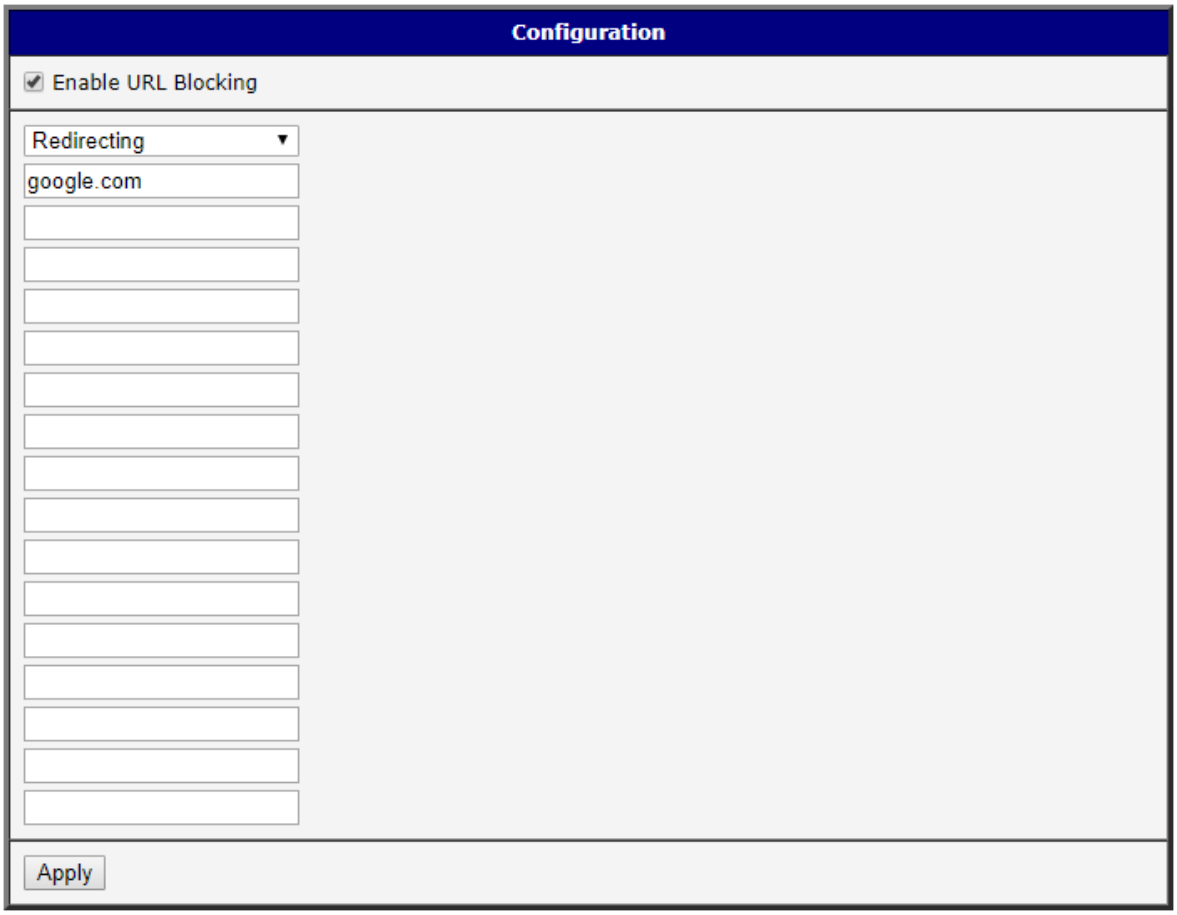


Figure 6: Example of redirecting mode

In this mode the default Welcome/Banned page will tell the user the page is blocked as you can see in the Figure bellow:

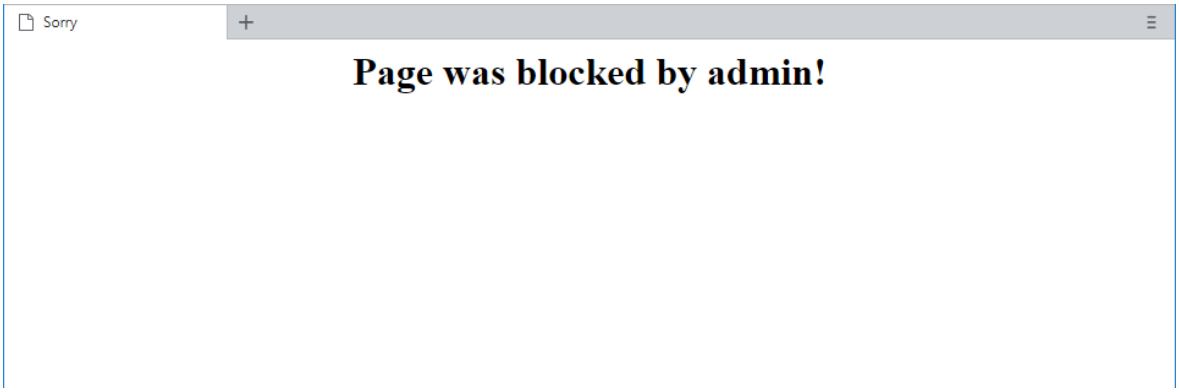


Figure 7: Default information page after redirection

You can prepare your custom Welcome/Banned page and upload it to the user module on *Welcome/Banned Page* in the *Configuration* section.

Requirements for the upload are the following:

- The uploaded file has to be an archive in **.tgz* or **.tar.gz* format (tarred and gzipped file). It can be done by native utilities in Linux or by e.g. 7-Zip application in Windows (freeware, take two steps: tar and then gzip).
- There has to be an *index.html* file in the root of the archive (no folder).
- The size of the archive has to be *1.5 kB* or less.

Choose the prepared file on the *Welcome/Banned Page* and click the *Update* button:

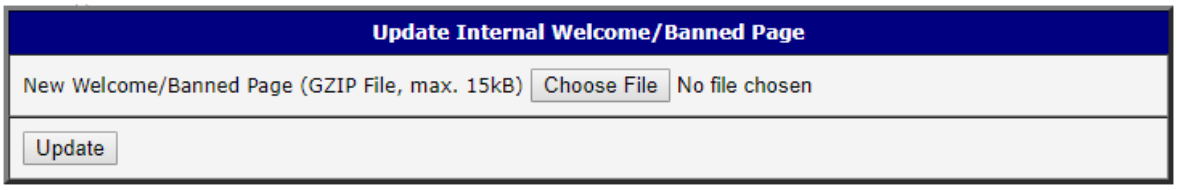


Figure 8: Upload custom welcome/banned page form

See the result of the successful upload in the next Figure. The uploaded page will be then shown to the user when the domain is blocked in the *Redirecting* mode.

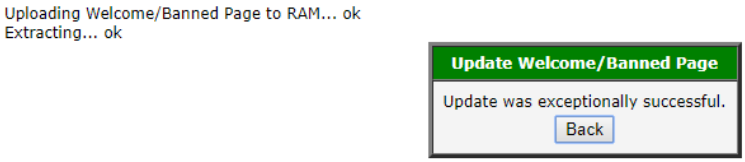


Figure 9: Successful upload of custom welcome/banned page

3. Recommended Literature

[1]	Advantech B+B SmartWorx:	**v2 Routers Configuration Manual** (MAN-0021-EN) available from: https://ep.advantech-bb.cz
[2]	Advantech B+B SmartWorx:	**SmartStart Configuration Manual** (MAN-0022-EN), available from: https://ep.advantech-bb.cz
[3]	Advantech B+B SmartWorx:	**SmartFlex Configuration Manual** (MAN-0023-EN), available from: https://ep.advantech-bb.cz
[4]	Advantech B+B SmartWorx:	**SmartMotion Configuration Manual** (MAN-0024-EN), available from: https://ep.advantech-bb.cz
[5]	Advantech B+B SmartWorx:	**ICR-3200 Configuration Manual** (MAN-0042-EN), available from: https://ep.advantech-bb.cz
[6]	User Modules – Engineering Portal:	**https://ep.advantech-bb.cz/user-modules**