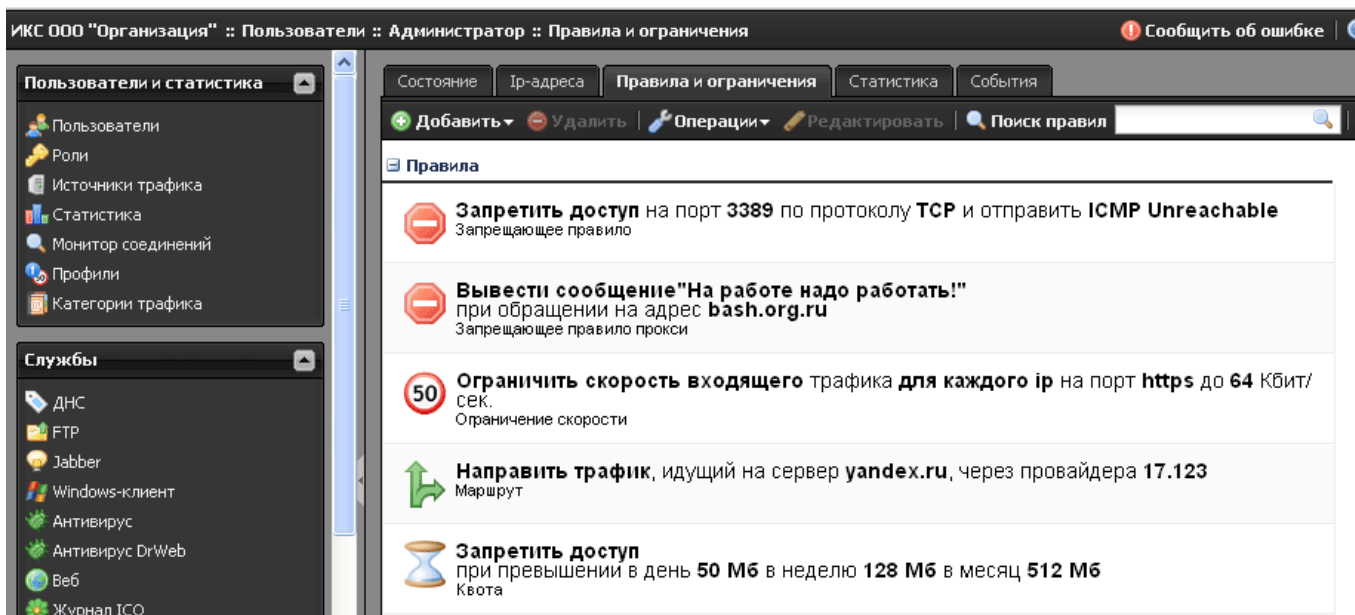


User Access rules

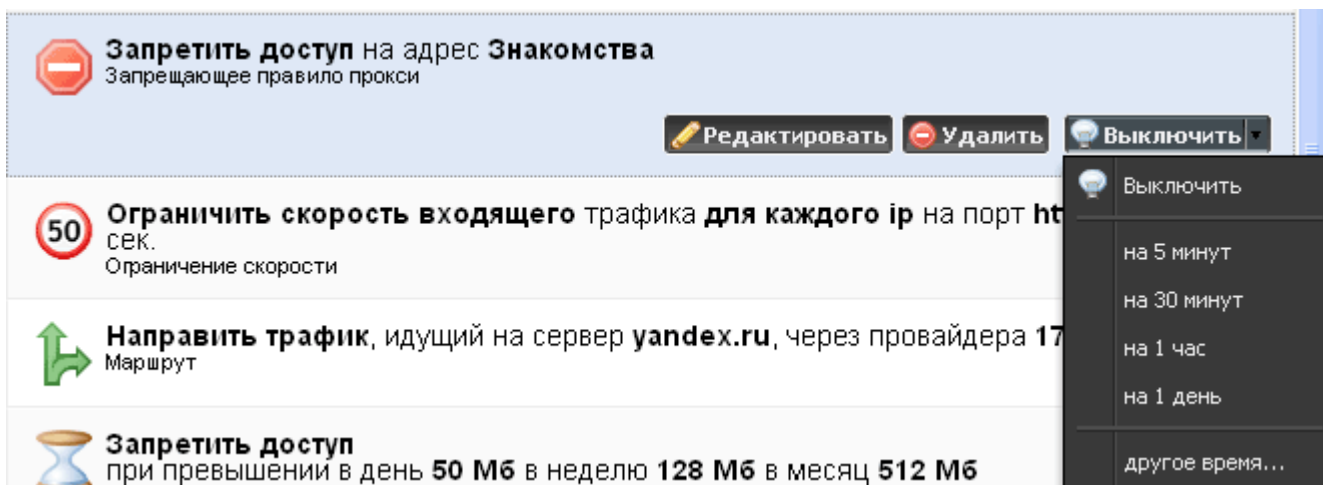
General

In order to assign an access rule to user or group click user or group name in module users. User (group) profile page will be displayed. Go to tab “rules and restrictions”, click “add” and choose the necessary type of rule.



All created rules are displayed as a list in “rules and restrictions” tab. Their order is irrelevant.

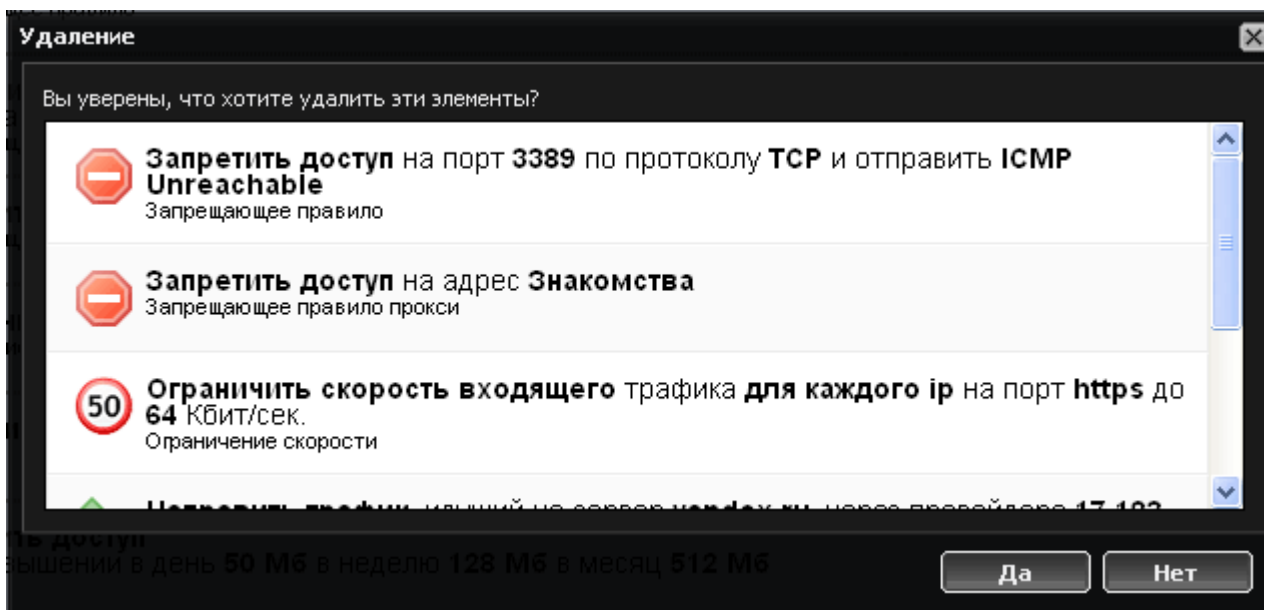
Action rules



If you click a rule in the list, in the upper right corner you will see three possible actions for that rule: edit, delete, switch off. Option “switch off” has a drop down menu that allows you to switch off the rule completely or choose a time period.

Group actions

To delete or switch off several rules simultaneously, highlight them in the list holding down CTRL (one by one) or SHIFT (as a list). Then in the upper panel choose the action to be applied: delete or edit (possible for a time period).



A confirmation window will pop up. Click “yes” to confirm, and “no” if you want to add corrections.

Types of access rules

In user or group “rules and restrictions” tab you can assign the following restrictions to users:

Deny rule - adds a deny rule to firewall, works for IP addresses, ports and protocols, allows you to block any host in external or internal network.

Allow rule - adds an allow rule to firewall, used to create exceptions to deny rule

Proxy deny rule - adds a deny rule to server proxy settings, works for URL, allows to block individual domains, pages and its elements through regular expressions.

Proxy allow rule - adds an allow rule to server proxy settings, used to create exceptions to deny proxy rule.

Connections limit - allows limiting number of user's connections to defined resource, protocols or ports.

Speed limit - allows limiting the speed of user’s access to resources, protocols or ports.

Bandwidth allocation - allows managing policies prioritizing traffic for faster access to necessary sources.

Quota - assigns a daily, weekly or monthly traffic on defined address, protocol or port to a user..

Route - adds a static route for a user.

DLP control - adds a rule which will scan the user's traffic according to signature database [DLP](#).

Content filtering rule - adds a proxy rule which checks loaded html-code and compare it to signature database [контент-фильтра](#).

Profile - adds a profile access to a user with a combination of various rules.

From:

<https://doc.a-real.ru/> - **Документация**

Permanent link:

https://doc.a-real.ru/doku.php?id=en:user_access_rules50

Last update: **2020/01/27 16:28**

