Setting up HTTPS-filtration

For obtain the opportunity to filter HTTPS-traffic, you should perform these steps:

1. Create root certificate with default settings (CA) in the “Certificates” module

For certificate to work for a long time without replacement, set the expiration date that is longer than a year (by default). Other fields leave by default.

After you press the “Add” button, the system will ask whether you need to encrypt private key. Choose “Do not encrypt private key” option.

2. Choose this certificate in the “Certificate for HTTPS filtering” field of the Proxy module.

Afterwards you can choose one of the two modes of filtration process:

Filter HTTPS traffic with decryption. In this mode all traffic will be decrypted using certificate substitution. Using this option, you’ll get all filtration rules to work, but, in case of certificate substitution browsers will display warnings about incorrect certificate. To fix this issue, the following can be done: From the “Certificates” module the certificate should be exported to a workstation. You don’t need to export certificate key with it.

For each workstation certificate should be added in the trusted root certification authorities store. Here’s some instructions (at the example of Windows 7): double-click the certificate. Choose the “install certificate” button. The Certificate Import Wizard would be launched. When the wizard would ask you about the store for this certificate, select «Place all certificates in the following store», click Browse, and choose the “Trusted Root Certification Authorities store”.

After these actions, the certificate will be imported in the global system store. It will work for browsers that use system certificates store, for example, Internet Explorer, Chrome, Yandex. If a browser uses its own store, like, for example, Firefox, than you'll have to import certificate into this browser. For Mozilla Firefox you can do it this way:

Enter the Preferences menu, choose Advanced – Certificates – View certificates – Import and then choose the certificate that you downloaded from ICS.

Mark all the checkboxes and import the certificate.

For exclude some users or domains, you can use the field “Exceptions”. The sessions of users, who are specified in this field, would not be decrypted, and, therefore, you have no need to import certificate to their computers. It works the same way for the domains – the sessions with them would not be decrypted. For example, you may need to add domain in this field for precise work of secure services that check for MitM-attackes, like mail or bank services.

Filter without certificate substitution. In this mode you don’t need to implement a certificate to workstations. But this way ICS would only know about destination domain, but not whole address. For example, you can choose filtration without certificate substitution if you want to just block the whole “yandex.ru” domain. But if you want to block “yandex.ru”, but permit “yandex.ru/video”, then you need to assemble certificate substitution for decryption of the destination.

Also, in this mode you can set up full decryption for any domain and any user in the field “filter with decryption”. If you set it up for a user, you should import your certificate to his workstation, and if you set it up for a domain, you should import your certificate to all workstations that will address this domain (for example, vk.com).