Proxy

Main page of the module

Proxy-server is the service that helps its clients to make indirect requests to other network services. The client connects to a proxy-server and make a request for some web-resource, located in the other server. Then proxy either connects to the required server and receive some response from it, or returns some response from its own cache (if any client has requested this resource already). In some cases client request and server response can be altered by proxy for some purposes.

Also, proxy-server can analyze clients HTTP-requests that go through it, perform filtering functions and account traffic using mime-types. Above all, proxy-server allows to set up internet access using login/password pair.

Proxy-server also caches objects, received by users from internet, and through this reduces traffic usage and increases connection speed.

At the entrance to the module you can see service status, “Disable” (or “Enable” if the module is currently off) button and recent log messages.

Settings

Usually to use proxy you should specify its address and port in the browser options. But if you don’t need to authenticate users by login/password pair, you can use “transparent proxy” function.

In this case all HTTP requests from the local network will automatically go through proxy-server. So, you’ll have an oportunity to filter and count traffic despite settings on local machines.

Default proxy-server port is 3128, but in the “settings” you can specify whatever port you like.

Authorization types

ICS proxy-server allows two ways of authorization: through user ip-address and through login/password pair.

Authorization through ip-address is useful, when employee uses the same computer constantly. Prozy defies the owner of the traffic through the ip-address of his computer. This is not the way for terminal servers, because in this case many users share the same ip-address. Also it is not the way for organisations, where employees don’t have a permanent work place. Above all, the user can change his ip-address, and, if you didn’t set up binding between MAC and ip-addresses, ICS will consider him as someone else.

Login/password authorization resolves the problem of linking user to a computer. In this case, when user sent first request, browser will show login/password form, which he must fill for have access to internet. If you have domain authorization in your network, you can choose “domain authorization” option. In this case, if ICS is connected to the domain controller, and users were imported from this domain, authorization will be transparent to users, and browser would not ask them for login and password.

This way has a disadvantage: it doesn’t work with transparent proxy, so, in all software that use internet, proxy address should be entered manually.

Above all, you should remember, that proxy authorization is used only for http-traffic. Internet access for software which use other protocols, is regulated by firewall, and firewall can authorize only by ip address. In other words, if employee use only login/password authorization, he couldn’t use mail, or jabber, or torrent-client, and other programs which cannot use http-proxy.

Web-authorization

If you want to authorize users without specifying proxy-server, but using login/password authorization, you can use “web authorization” (captive portal) by marking the checkbox. Web-authorization can, for example, integrate authorization page with the company portal, and use it as an authorization page. Default web-authorization port is 82, but you can choose any unused port you like.

When entering the page http://ip_ics:82 you will see this kind of message:

Also, if you turn web-authorization on, then non-authorized users will be automatically redirect to the authorization page.

For log out, the user can use the same authorization page and press the button “log off” there.

Checkbox “from one ip-address only” forbids several users to connect using the same login.

User, authorized this way, will have access to all protocols (not only HTTP), according to rules and restrictions made for him.

SMS-authorization

There is an opportunity to use sms-authorization in ICS.

How does it work:

1. The user connects to your Wi-Fi spot.

2. The user opens browser, enter his mobile number, and press the “Receive the code by SMS” button.

3. User receive SMS with a code to this mobile number.

4. User enter this code to the authorization field and then he would have access to internet.

For now ICS uses the “SMS.RU” service for sending sms.

We plan to add other sms services soon. If you are interested in any particular service of this kind, you can write to us, and if it would be possible, we’ll try to add it to ICS.

Use SMS-authorization – turns on SMS-authorization.

SMS-authorization port – port, which is listening for the income connections for access to the authorization web-form.

ID – the secret key you gain from the SMS.RU site.

You can find this key right on the main page of you profile at the sms.ru, bottom-right:

Assign an address to a user – the ICS user, to whom will be passed the IP-address of a client that have successfully passed SMS-authorization.

Page caching

Proxy-server performs caching of the web-pages and objects that users download from internet. This way you can reduce traffic and increase speed when surfing web- pages through ICS.

The efficiency of cache is depending on its size. For the organization that has a lot of users, we recommend to set several gigabytes for cache (in the appropriate field). You can also limit download files size in the field “Answer size limit” (in Mb).

The option “Hide user’s IP-address” lets you turn off the mention of ip-address in the frame of the packet (forwarded_for parameter).

You can check cache content in the tab “cache content”. But you should remember, that web-interface doesn’t show all of the cache content, but only a part of it, like images.

Transparent proxy

In this mode instead of listening for users requests at the proxy post, ICS redirect them all to the proxy itself. The proxy-server processes the request (using cache whenever possible) and sends content back to the user. For user it looks like he is getting the answer from the server he had requested. In this model, user can even be unaware that his traffic goes through proxy-server. By default, transparent prozy listens to 80 port (HTTP).

You can define, whether to turn on or off the transparent proxy for DMZ and LANs, using appropriate checkboxes in settings menu. By default transparent proxy is turned off for DMZ and on for LANs.

There are some programs that can turn suspicious when they notice proxy interference. You can add their addresses in “Transparent proxy exceptions” and theirs traffic won’t be processed by proxy.

For implementing HTTPS-filtration you should fill the “SSL-filtration certificate” field with previously created root certificate. All addresses that should not be filtered with this certificate, they may be added to exceptions.

SOCKS5

SOCKS is a network protocol that allows client-server applications to use transparently the services that are located behind a firewall. When a client from behid a firewall needs access to an external server, he can connect to SOCKS proxy-server instead. That kind of proxy-server controls client access rights for external resourses and redirect requests to the server. SOCKS can be user contrariwise, giving access rights for connection to the servers behind firewall.

Unlike HTTP proxy-servers, SOCKS redirects all client data without altering it. So, from the perspective of the target server, SOCKS-proxy is just an ordinary client. SOCKS is more versatile – it is not dependent on application protocols (level 7 of OSI/ISO model) and is based on TCP/IP standart – level 4 protocol. But HTTP proxy can cache transmitted data and filter them more thoroughly.

You can use SOCKS5-server as a part of proxy-server for non-HTTP protocol authorization. By default the access port is 1080, but you can change it if you like. It uses ip-based authorization, but, filling the appropriate checkbox, you can initiate login/password authorization.

Anti-virus

Internet Control Server can analyze traffic that passes through proxy-server with anti-virus. In the 5th version of ICS there are 3 anti-virus modules: free anti-virus ClamAV and non-free - DrWeb and Kaspersky. For antivirus to start working, the license should be purchased and installed in the module.

Also, for turning on antivirus analyze for web-traffic (by any of these modules), it’s necessary to turn on this option in proxy settings. The “maximum size parameter” defines maximum size of a file, that passes through anti-virus. All files that are bigger that this, would not be scanned, and it can sufficiently increase efficiency.

It’s recommended to turn on images analysis, cause there are viruses, that use ordinary pictures, but scanning pictures as usual increase system resource usage by the anti-virus, and when a lot of pictures are processing, performance of the server can be reduced.

Allowed ports

You can choose, through which ports clients are allowed to connect to external servers using proxy. The list of allowed ports for SSL defines, which ports are allowed for access using the CONNECT method.

ICAP

ICAP (Internet Content Adaptation Protocol) – is the protocol for extended proxy functions. In most cases it is used for virus scanning of traffic and for applying different content-filters. You can add an external ICAP-server in ICS, by filling the checkbox in settings and entering its address.

Three last checkboxes will turn on DLP and content filter, and SkyDNS respectively.

Proxy autoconfiguration

If you don’t want to set proxy address on each workstation, you can use autoconfigurator. In this case in user’s browsers an option “auto-detect proxy” setting must be chosen, and all the rest will be done by ICS.

It can be turned on with checkpoints in this tab. You can mark one or several of available protocols (HTTP, HTTPS).

The script public option is defining whether it would be available on the server ip-address, or on the virtual host with a domain name. When you choose virtual host, it would be created in the system automatically. By marking the “Create dns zone” checkbox you’re instructing ICS to add automatically the zone and all domain names that are necessary for this virtual host.

Public autoconfiguration script by DHCP – this parameter sent proxy settings to all DHCP-clients of the server.

Parent proxy

If there is several proxy-servers in your organization and they have hierarchy, then the one that is standing on top of ICS would be a parent proxy for him. Also, any node can act as a parent proxy as well.

For ICS to redirect requests, that are coming to his proxy-server to the parent proxy, you can enter its ip-address and destination port in the “Parent proxy” tab.

Proxy-servers can use ICP protocol for cache exchange. In case you’re working through several proxy, it can significantly increase efficiency. If your parent proxy supports this protocol, you can mark the related checkbox and define a port for this service (by default it’s 3130).

If you parent proxy requires authorization, you can enter login and password in the fields below.

Issued ip-addresses

In this tab you can find the list of ip-addresses and users, who has been authorized in proxy-server using web-authorization.

Cache content

In here you can look at some elements of web-pages (mostly pictures), which are stored in cache, and also you can clear cache completely.

Log

In “log” tab is located summary of all proxy service log. It is divided to several pages, you can use “next” and “previous” buttons for navigation or enter page number to go directly to it.

Log messages differ in color depending on its type. Ordinary messages are white, system condition messages (turning on/off, cache processing) are green, and errors are red.

In the right top corner the search is located. You can use it to find anything you need in the log.

Log always shows current day events. If you want to see log from another date, just choose the date you need, using the calendar in the left top corner of the module.

From:
https://doc.a-real.ru/ - **Документация**

Permanent link:
https://doc.a-real.ru/doku.php?id=en:proxy50

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