УДК 621.391

Kaptur V.A.
Каптур В.А.
Каптур В.А.

CENTRALIZED SYSTEM OF HTTP-TRAFFIC FILTRATION

ЦЕНТРАЛІЗОВАНА СИСТЕМА ФІЛЬТРАЦІЇ HTTP-ТРАФІКА

ЦЕНТРАЛИЗОВАННАЯ СИСТЕМА ФИЛЬТРАЦИИ HTTP-ТРАФИКА

Summary. The basic construction principles of the centralized system of http-traffic filtration based on proxy-server are proposed. The possible options for redirecting of http-traffic to the centralized filtration system are reviewed. Practical recommendations for network administrators on the connection of networks of different types to the proposed system are given.

Анотація. Запропоновано базові принципи побудови централізованої системи фільтрації http-трафіка на основі proxy-сервера. Розглянуто можливі варіанти переспрямування http-трафіка до централізованої системи фільтрації. Наведено практичні рекомендації для мережних адміністраторів щодо підключення мереж різних типів до запропонованої системи.

Аннотация. Предложены базовые принципы построения централизованной системы фильтрации http-трафика на основе proxy-сервера. Рассмотрены возможные варианты перенаправления http-трафика к централизованной системе фильтрации. Приведены практические рекомендации для сетевых администраторов по подключению сетей разных типов к предложенной системе.

Increasing rates of global information society caused by the implementation of several legislative acts, national task programs and grants for the equipping of educational institutions (schools, universities, etc) with computer means and connecting to the Internet network, set the world community a new challenge - the necessity of secure access organizing to the information resources of the Internet for pupils and students. As you know the Internet (in its major part) is practically unregulated and filled with a wide range of information which is placed on various information resources: from scientific magazines to those that are directly promoting violence, contain inappropriate language and / or are openly pornographic. Under these conditions, support of appropriate cultural level and morality in society is almost an unrealizable task.

There are different views on the regulation of situations with morality questions, pornographic resources, personal life and data privacy in different parts of the world and different technologies used for restriction of access to inappropriate Internet content. The most popular technologies are: blocking by IP-address using means of firewall on the router or workstations [1]; Web browsers' embedded functions to restrict access [2]; proxy-servers located within the organization's network [3]; filtering resources on the DNS servers [4]. All of listed methods are possible in use in a centralized or decentralized scheme.

In Ukraine (on the basis of Odessa National Academy of Telecommunications n. a. O.S. Popov) the system for restricting access to inappropriate Internet content in educational institutions (schools, universities, etc) based on decentralized scheme [5,6] has been created. Setting of own proxy-server that has a database of inappropriate resources in each educational institution is the basis of the principle. For the purpose of continuous update, processing of log-files of mentioned servers is centralized; these servers based on the information center with subsequent periodic formation of an updated version of the banned resources database and sending it (automatically) to all proxy-servers introduced.

The main advantages of this system is the simplicity of scalability, reliability and adaptive filtering of negative content, significant reducing of the overall http-traffic due to the caching of information (reducing the cost of exploitation of access channels), adjustment to the emergence of new inappropriate resources.

However, one of the most serious disadvantages of decentralized systems is the high cost of its use (it is needed to purchase additional equipment to install a proxy-server in each organization). This approach can be fully justified if organization has more then ten workstations, but is redundant for organizations with less than ten computers.

Purpose of the article - the development of the concept of centralized system of http-traffic filtration.

Generalized scheme of the centralized system of traffic filtering is shown in Fig. 1. Hierarchical system is composed of the core and objects (schools, private companies, etc.). Filtering can be based on individual settings, which are made by network administrators of any organizations connected to the system via web interface.

Http-traffic for filtration routed between objects and core via the Internet. The system provides different ways to connect objects to the core:

– by blocking access by means of firewall to any hosts except proxy (installed in core of filtration system) with modification settings of proxy-server in each web-browser in organization;

– by redirecting of http-traffic on router to the core by means of firewall settings. Network administrator can use firewall rules for redirection of http-traffic to proxy-server (using IP & port);

– by forwarding of all http-requests from the organization's proxy-server to the core proxy-server;

– by creation of network tunnels to the core of the centralized system of traffic filtering, etc.

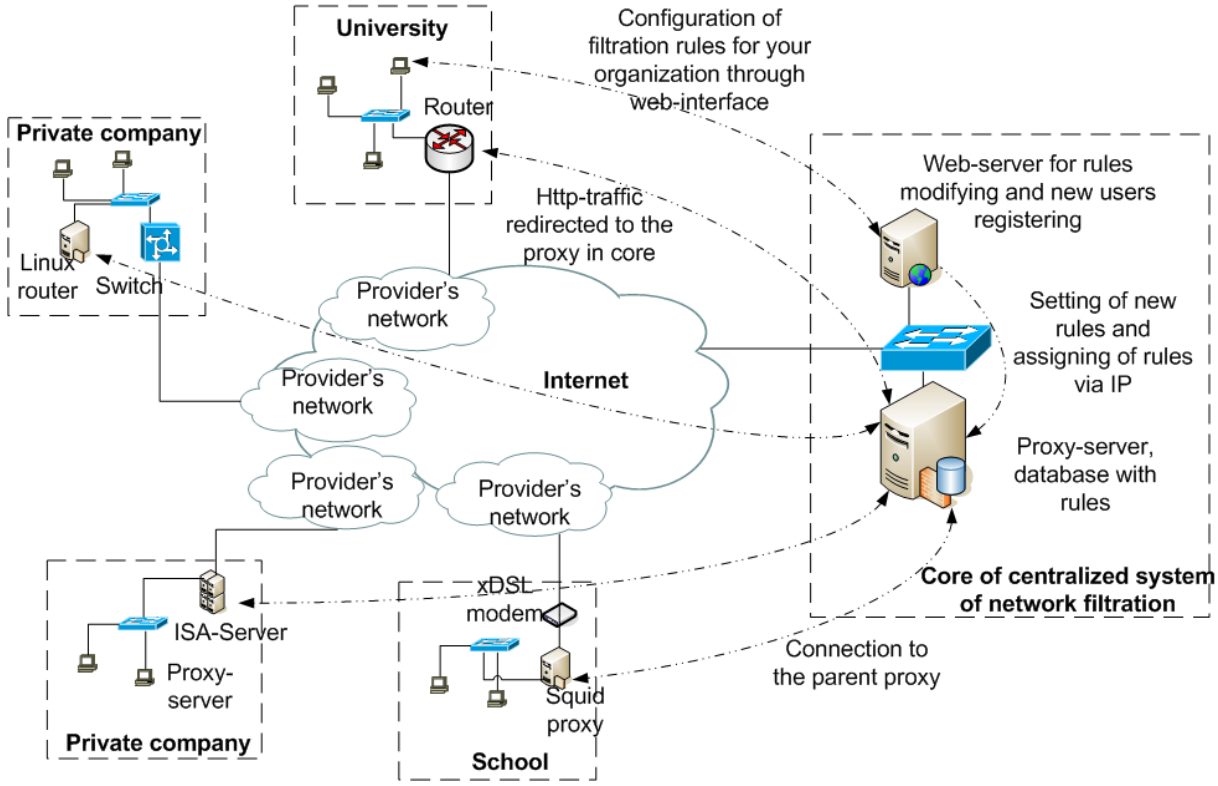

Figure 1 – Scheme of the centralized system of traffic filtering

The generalized scheme of interaction of the network with any object connected to the system via core filter is shown in Fig. 2. This interaction is based on redirection of http-traffic to the system core.

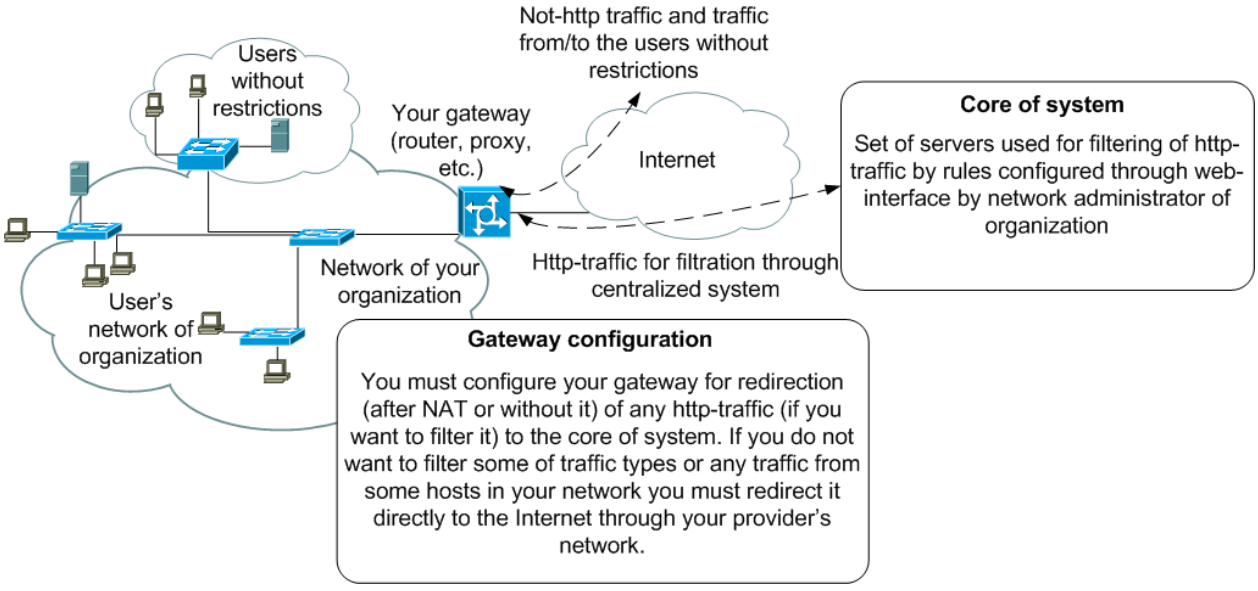

Figure 2 – Scheme of interaction in you network

Fig. 3 shows the algorithm of user's interaction with the Internet and filtration system.

The decision to redirect the traffic of any hosts of the computer network to the core is adopted by the network administrator. If it is necessary, the administrator can send traffic of some hosts (such as a teacher's computer) directly to the Internet (without filtration), and the traffic of all other hosts is automatically redirected to the core of filtration system.

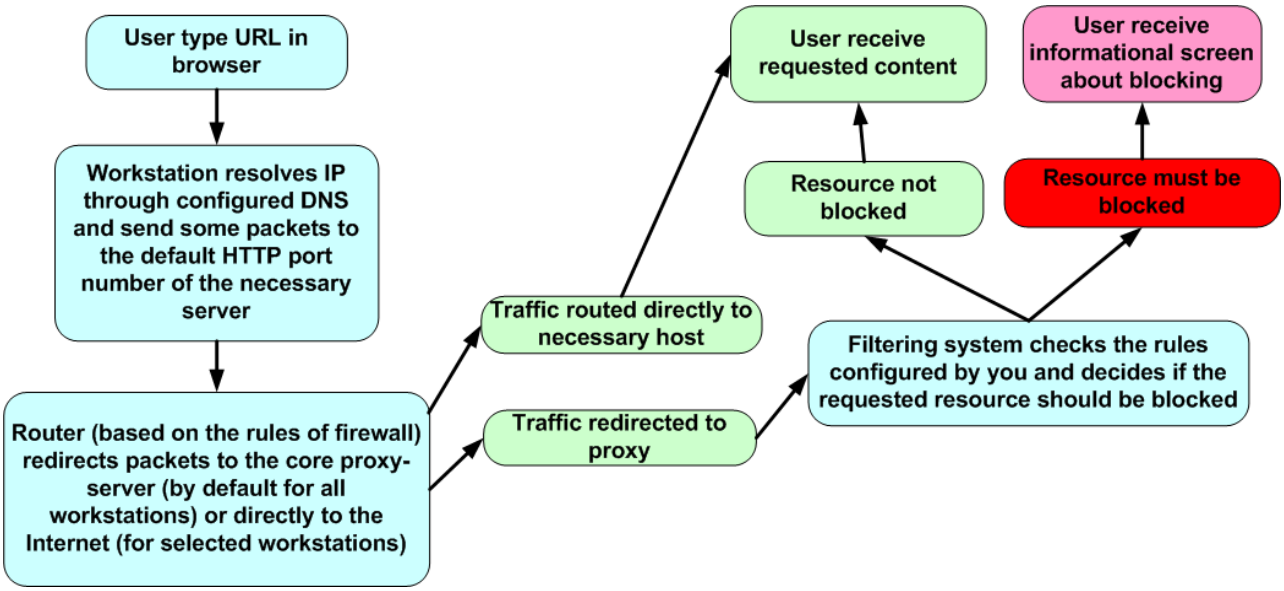

Figure 3 – Algorithm of user interaction with filtration system

After request of any URL (using any browser) the user's workstation attempts to connect to the necessary server on the Internet. Gateway of organization according to settings can redirect all IP-packets to the proxy-server located in the core of filtration system or directly to the requested server in the Internet.

Filtration system determines the IP-address of the host (or network) that sent the HTTP-request and according to filtering rules (made by network administrator) checks and carries out a decision to block access (or not). In block case: instead of the requested resource user receives a message that may contain some advertising information.

Filtration system can be used for any workstation of the network regardless of operating system or software which is used for Internet access. The only requirement for all objects that are connected to the system is the presence of a gateway or proxy with firewall for redirection of traffic to the system core. If organization don't have separate gateway (or the gateway does not support firewall with redirection function or NAT) – it must be additionally installed.

All corporate networks of educational institutions can be divided into two types: networks based on a gateway and networks without gateway (e.g. SOHO-modem based networks). The second type (in most of cases) requires the full modernization of the network. The first type has several different variants for network construction. The most popular variants of network architecture of first-type networks: router based networks and proxy-based networks.

Configuration of traffic redirection (for any variant) depends on the type of network operating systems (* nix, Windows, etc) and the versions of used software. Configuration templates for various operating systems listed in Table 1.

The proposed architecture of filtration system has several significant disadvantages:

– equipment must have necessary productivity (not to make a big delay);
– the central node must have a large bandwidth of communication channels;
– in the case of the central node failure all system is down too.

Possible way to overcome these disadvantages is the developing of mathematical models of filtration systems to define the boundary parameters of its productive capacity. This model will be discussed in subsequent publications.

Table 1 – Configuration templates for various operating systems

#	OS type	Configuration template (manual)
1	Linux	Linux kernel must be compiled with netfilter and NAT support. Userspace utility "iptables" must be installed and configured using the following template: "iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination proxyIP:proxyPortNumber".
2	FreeBSD	FreeBSD (using ipfw2) network administrator can use following template: "ipfw add 1000 fwd proxyIP,proxyPortNumber tcp from any to any 80 in recv $int_if". FreeBSD (using pf) must modify content of "pf.conf" with using following template: int_if="em0" ext_if="em1" rdr on $int_if inet proto tcp from any to any port www -> proxyIP port proxyPortNumber pass in on $int_if inet proto tcp from any to proxyIP port proxyPortNumber keep state pass out on $ext_if inet proto tcp from any to any port www keep state
3	Cisco IOS	Cisco IOS configuration can be realized using the following sequence of commands: "enable; conf t; ip nat inside destination static tcp <ip_to_forward_from> 1980 proxyIP: proxyPortNumber extendable".
4	Windows	For redirect http-traffic to centralized system of traffic filtration in Windows administrators can use the freeware version of Routix NetCom software (http://www.routix.net/netcom/) or any of its analogue.

Conclusions and recommendations

1. The question of restricting access to inappropriate Internet content today has become one of the most important in modern society.

2. Deployed in ONAT n.a. O.S. Popov decentralized system of restricting access has a number of advantages, but its implementation requires a rather significant investments.

3. Using a centralized system of http-traffic filtration can be an optimal choice for organizations with few workstations.

4. The proposed system architecture and recommendation for configuration subscriber's routers can help to extend the system of restricting access to any entity that has access to the Internet.

References

1. *Microsoft* Corporation. How to Configure Windows Firewall in a Small Business Environment Using Group Policy. [Electronic resource]. – Access mode: http://technet.microsoft.com/en-us/library/cc875816.aspx#EBJAC
2. *ICRA* filtering using Microsoft Internet Explorer. [Electronic resource]. – Access mode: http://www.icra.org/support/contentadvisor/setupv03/.
3. *Squid-cache* wiki. Blocking Content Based on MIME Types. [Electronic resource]. – Access mode: http://wiki.squid-cache.org/
4. *Project OpenDNS*. [Electronic resource]. – Access mode: http://www.opendns.com/solutions/overview/
5. *Воробієнко П.П.* Єдина система обмеження доступу до нецільових ресурсів мережі Інтернет в освітніх закладах України [П.П. Воробієнко, В.А. Каптур, В.А. Коляденко, В.О. Самодід] // Комп'ютер у школі та сім'ї : науково-методичний журнал/ Інститут педагогіки АПН України. – Київ. – 2009. – №8. – С. 30-34
6. *Kaptur V.A.* System for restricting access to inappropriate Internet content in educational institutions (schools, universities, etc) and hostels // First meeting of the Council Working Group on Child Online Protection (CWG-CP), Geneva, 17-18 March 2010