XXXI Неделя науки СПбГПУ. Материалы межвузовской научной конференции. Ч. VII: С. 38-40, 2003.

УДК 681.3.06.

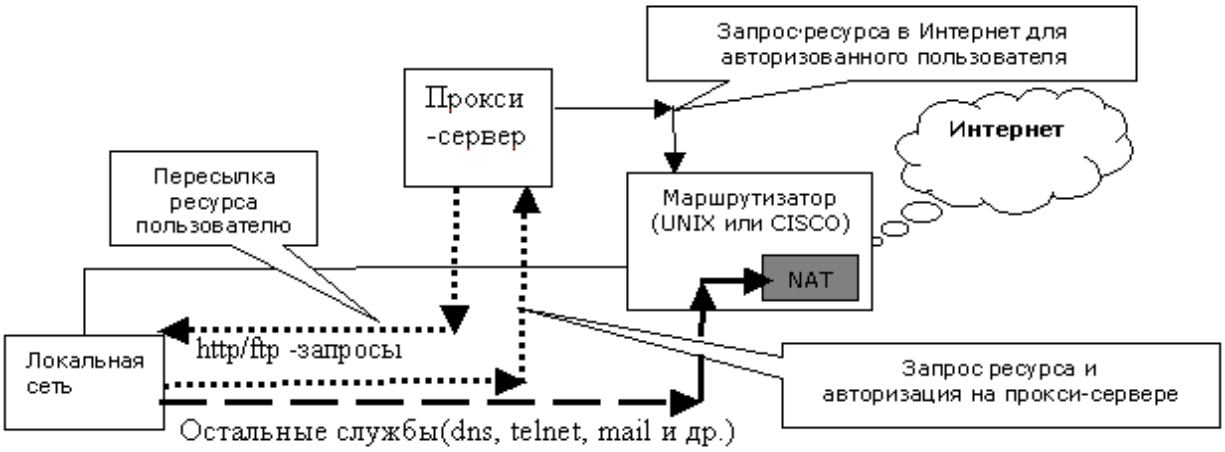
Н.Ю.Новикова (6 курс, каф. РТТК), Д.Ю.Новиков, ЗАО «Ниеншанц», СПб

ПРОКСИ-СЕРВЕР — ИНСТРУМЕНТ ГИБКОГО УПРАВЛЕНИЯ ДОСТУПОМ ПОЛЬЗОВАТЕЛЕЙ К ИНТЕРНЕТУ

ABSTRACT: There are results of researches access system for network corporate users to the Internet through a Proxy. The program proxy SQIUD controlled OC Unix have been learned. The technologies of authorization through the external program have been investigated. Is was developed the technology of authorization through the SQIUD-server the of the Windows domain controller accounts.

Представленная работа относится к тематике авторизации пользователей корпоративной сети при доступе к ресурсам Интернета. Проблема заключается в том, что основные приемы авторизации, например, через брандмауэр, позволяют авторизовать пользователей строго по IP-адресам их рабочих мест. Однако возникают ситуации, когда пользователь не связан с рабочим местом, и, соответственно, с IP-адресом компьютера, например, при работе в терминальном режиме. И тогда приходится внедрять другие схемы авторизации — по входному имени (логину) и паролю пользователя. В работе представлена система авторизации пользователей посредством ПРОКСИ-сервера через внешнюю программу по Windows-бюджетам.

Доступ к службам Интернета на многих предприятиях реализуют через сервер, управляемый ОС UNIX. Практически всегда для Web- и FTP- трафиков используют кэширующий сервер — ПРОКСИ-сервер (программа SQUID). Обычно он подключается совместно с аппаратным маршрутизатором или UNIX-сервером, так, как показано на рисунке.



Стандартный способ доступа к ПРОКСИ-серверу — через специализированные списки доступа (Access Lists или ACL). Эти списки обычно строятся на основе IP-сетей, которым разрешен доступ к SQUID. С помощью списков доступа можно разрешать или запрещать доступ к Интернету компьютерам (или сетям) с определенным IP-адресом. К тому же, при использовании Интернет-ресурсов, в лог-файл SQUID записывается информация о конкретном адресе, запросившем конкретный Интернет-ресурс. Такая технология позволяет контролировать трафик по IP-адресу Интернет-пользователя. В большинстве случаев авторизация по IP-адресу вполне подходит, но требуется, чтобы за конкретным компьютером всегда работал определенный человек.

Случается, что пользователи не связаны с конкретным IP-адресом, например:

1. Работа разных людей на одном и том же рабочем месте (например, посменно);
2. Сотрудник пользуется разными компьютерами (садится за освободившийся);
3. Работа в терминальных сессиях терминального сервера (в этом случае весь Интер-

нет-трафик идет с IP-адреса сервера).

Поэтому актуальна проблема учета трафика не на основе IP-адресов, а на основе другой информации. Логичным решением является авторизация в SQUID по логину и паролю. В ПРОКСИ-сервере возможна авторизация через внешнюю программу, которая адекватно реагирует на ввод логина и пароля. Поэтому удается производить авторизацию по учетным записям на UNIX-сервере через текстовые файлы. Но такая авторизация осложняет работу пользователей и администраторов. А именно:

1. Для доступа к Интернету приходится вводить в броузере логин\пароль;
2. Администратору необходимо вести базу логинов и паролей в специальном файле.

Для решения этих задач авторами разработана система авторизации ПРОКСИ-сервером по Windows-бюджетам. Известно, что в Windows-сетях каждый пользователь при входе в сеть проходит авторизацию в NT(2000)-домене. Если использовать эти данные для авторизации, можно решить проблемы ведения в SQUID отдельной базы данных пользователей и запроса логина\пароля в браузере при входе в Интернет. Главное здесь — подобрать и настроить программу авторизации определенного пользователя в Windows-домене. Разработчики SQUID рекомендуют пользоваться программой winbind из пакета SAMBA (эмуляция Windows-сервера и клиента под UNIX).

Практическое решение задачи было получено программным путем. Программа авторизации была сконфигурирована, настроена и внедрена в большой корпоративной сети. В итоге получилась гибкая система авторизации с перечисленными ниже свойствами.

1. Если пользователь авторизовался в домене, то IE не запрашивает пароль. Пользователь сразу попадает в Интернет, а информация о нем заносится в лог-файл SQUID.
2. Если пользователь не авторизовался в домене — происходит запрос логина и пароля. При совпадении данных с Windows-бюджетом, пользователь попадает в Интернет.
3. При использовании браузеров Mozilla, Netscape, Opera пользователь обязан вводить логин и пароль для авторизации.
4. Если аккаунт в Windows-домене закрыт, доступ в Интернет также будет закрыт.

Работы по изучению и внедрению ПРОКСИ-сервера выполнялись на базе корпоративной сети крупной фирмы. В результате исследований получены важные практические результаты:

1. Установка ПРОКСИ-сервера позволила администраторам сети контролировать HTTP-трафик пользователей. Администраторы получили удобный инструмент для управления доступом конкретных лиц к конкретным ресурсам. Это решило проблему непродуктивного присутствия в Интернете и, как следствие, уменьшило затраты на Интернет-соединения.

2. Удалось организовать учет трафиков по логинам и паролям Windows-пользователей сети. Это позволило, в том числе, решить проблему авторизации и учета трафика для пользователей, работающих в терминальных сессиях на одном сервере.

3. Выяснилось, что внедрение ПРОКСИ-сервера позволяет экономить порядка 30% трафика при кэш-массиве, составляющем объем 15 Гб.

ПРОКСИ-сервер прошел успешные испытания в октябре 2002 года и в настоящий момент вводится в коммерческую эксплуатацию.