XXX Юбилейная Неделя науки СПбГТУ.Материалы межвузовской научной конференции. Ч.VIII: С.29-30, 2002.
УДК 681.3.06.

Н.Ю.Новикова (5 курс, каф. РТТК),Д.Ю.Новиков, сотр. ЗАО «Ниеншанц», СПб

СИСТЕМА УЧЕТА И УПРАВЛЕНИЯ IP-ПОТОКАМИ В КОРПОРАТИВНОЙ СЕТИ

ABSTRACT: There are the results concerning to the protected Internet-connection for corporate networks. The computer network controlled by UNIX-system FreeBSD. The system of accounting and management IP-traffic was constructed, tested and introduced. In the developed system was used the filters and counters build to firewall, and also the interface was written on Perl.

В России многие фирмы оборудованы локальными компьютерными сетями. Это позволяет сотрудникам фирмы работать с единой базой данных, пользоваться файловым хранилищем и сетевой периферией. На определенном этапе возникает необходимость подключения внутренней сети к глобальной сети Интернет.

При подключении локальной сети предприятия к Интернету неизбежно встает вопрос о защите от внешних атак. Основные мотивы, побуждающие устанавливать механизмы защиты корпоративной сети — сохранение корпоративных данных и противодействие нежелательному трафику. Дело в том, что подключенные к Интернету компьютеры попадают в «группу риска» — компьютер становится частью глобальной сети и доступен для IP-потока, инициированного удаленными системами. Таким образом, если нет противодействия атакам из Интернета, повышается вероятность проникновения «извне» к корпоративным данным. Вывод из строя или повреждение данных, хранящихся на компьютерах локальной сети, приводит подчас к полной остановке функционирования предприятия. Стоимость восстановления корпоративных ресурсов (базы данных и т. п.) высока и может заметно превышать затраты на установку средств защиты. К тому же, конфиденциальными данными могут завладеть нежелательные лица.

Поток паразитного трафика чрезмерно загружает канал Интернет-доступа. Характерный пример — процедура ICMP Flooding. Это «бомбардировка» из Интернета пакетами ICMP, которые забивают канал передачи данных, блокируя работу сети. Нечто подобное случается, когда одновременно из нескольких серверов на компьютер пользователя сети командой зондирования (ping) беспрерывно посылаются ICMP-пакеты.

Надежно защищает корпоративную сеть от атак из Интернета специальный механизм защиты — межсетевой экран firewall (его также называют брандмауэр). Он устанавливается на сервере, связывающем локальную сеть с Интернетом. Межсетевой экран выполняет не только защитные функции — как удалось выявить в процессе исследований, он позволяет эффективно управлять доступом пользовательских машин к Интернету, разрешать или запрещать различные Интернет-службы для отдельных лиц, для группы пользователей, для всей сети.

Следующий актуальный вопрос — оплата доступа к ресурсам Интернета. В режиме постоянного подключения к Интернету оплата производится в соответствии с количеством информационного потока: корпоративная сеть - Интернет. Чтобы распределять платежи по отделам организации или по сотрудникам, своевременно исключить «лишние» и паразитные потоки, следует наладить учет всего потока, проходящего через сервер (через маршрутизатор).

Таким образом, актуальной является задача построения защищенной системы, позволяющей вести учет IP-потоков в корпоративных сетях, подключенных к Интернету.

Представленная работа является результатом исследований, относящихся к задаче построения защищенных корпоративных сетей, подключенных к Интернету. Исследования и тестирование вариантов разработки выполнялись на базе учебной компьютерной сети EECNet (сеть Центра электроники и схемотехники СПбГТУ) и

корпоративной сети ЗАО «Ниеншанц» (Санкт-Петербург). Сеть EECNet является прообразом двухуровневой корпоративной сети — шлюз в Интернет построен на основе операционной системы UNIX-семейства, коллективная работа обеспечивается операционной системой Windows NT. Такая архитектура способна поддерживать функционирование как совсем небольших, так и довольно крупных сетей, то есть является масштабируемой в широких пределах. Сеть ЗАО «Ниеншанц» — большая корпоративная компьютерная сеть, поддерживающая соединение с Интернетом и обеспечивающая коллективную работу более сотни сотрудников крупной организации.

В результате детального изучения различных сетевых операционных систем (Windows NT, UNIX) в части поддержки ими Интернет-служб, в основу построения системы учета и управления IP-потоками положено решение, базирующееся на ОС FreeBSD, известной системе UNIX-семейства. Опыт пробной эксплуатации подтвердил правильность выбора базовой операционной системы.

В процессе проведения исследований были изучены системы предоставления Интернет-доступа и Интернет-служб для рабочих станций локальной корпоративной сети: система маршрутизации и кеширования WWW- и FTP– запросов для UNIX-систем (SQUID) и система защиты (межсетевой экран, брендмауэр), входящая в состав системы FreeBSD. Брендмауэр системы FreeBSD был взят за основу построения системы защиты сети EECNet. В ходе исследований выяснилось, что брандмауэр можно эффективно использовать не только в защитных целях, но и для детального подсчета различных (отличающихся адресатами, протоколами, портами) потоков на тракте: локальная сеть – Интернет. А фильтрующие функции брандмауэра вполне можно применить для управления потоками.

На основе анализа разных вариантов построения систем учета корпоративных потоков и подсчета количества передаваемых данных было принято решение разработать собственную систему учета потоков и управления доступом к Интернету. Основу построения системы составили следующие ключевые разделы — формирование набора правил доступа, сбор статистических данных, их обработка и визуализация. Создание интерфейса взаимодействия с системой — довольно важный этап в работе, поскольку интерфейсом во многом определяется, насколько система в целом приспособлена к удобному оперативному взаимодействию с «рычагами» управления потоками и их учета. Интерфейс программировался на языке Perl.

Пробный вариант системы учета и управления потоками был построен и прошел успешные испытания в сети EECnet. Результаты работы (структура системы управления и учета, система задания правил для потоков, интерфейс управления и сбора данных) представлены в докладе. Испытания показали, что разработанная система успешно решает важную задачу: обеспечение управляемого и защищенного доступа пользователей локальной сети к информационным и коммуникационным ресурсам Интернета.

Система, опробованная и внедренная в учебной сети EECNet Центра Электроники и Схемотехники СПбГТУ, целенаправленно делалась так, чтобы ее можно было легко модифицировать для применения в сетях различного масштаба, внешний сегмент которых построен на ОС FreeBSD. В частности, система учета и управления была проинспектирована специалистами ЗАО «Ниеншанц» (Санкт-Петербург) и одобрена к внедрению в корпоративную сеть предприятия для учета Интернет потоков.