XXIX Неделя науки СПбГТУ. Материалы межвузовской научной конференции. Ч.VI: С.19-20, 2001.

Н.Ю.Новикова (4092/2, СПбГТУ), В.С.Синепол, проф.,
Д.Ю.Новиков, сотр. ЗАО “Ниеншанц”

ОБ УПРАВЛЕНИИ IP-ПОТОКАМИ В ДВУХУРОВНЕВЫХ СЕТЯХ

Двухуровневая архитектура сети стала классической для компьютерных сетей организаций самого различного профиля. Внутренний сегмент такой сети обеспечивает коллективную работу сотрудников фирмы, внешний сегмент обеспечивает защищенный шлюз в Internet для внутреннего сегмента. При проектировании таких сетей актуальными являются задачи защиты от несанкционированного доступа к данным организации, учет потребления корпоративными пользователями внешних IP-ресурсов, а также анализ структуры IP-потока. Решение этих задач часто реализуется на основе специализированных программно-аппаратных средств, стоимость которых составляет десятки тысяч долларов. Для относительно небольших предприятий эти расходы являются неприемлемыми. В то же время может быть предложено решение, позволяющее обойтись меньшими затратами, — а именно, использование системных средств некоммерческих операционных систем.

И защита сети, и учет потребления IP-трафика могут быть построены на основе анализа пакетов сетевого уровня. Анализ может производиться по следующим параметрам:

- IP-адрес источника/приемника;
- тип протокола;
- порты источника/приемника;
- интерфейс приходящих/исходящих пакетов.

При построении системы учета (биллинговой системы) важно знать полный поток по маршруту “Internet – сеть организации”. Эти данные можно получить, анализируя IP-поток через внешний интерфейс сети. Для выяснения более тонкой структуры трафика необходимо исследование всех IP-пакетов по соответствующим параметрам. Такой анализ является основой системы защиты, реализуемой посредством фильтрации входного (выходного) потока по определенным признакам (порт, адрес, протокол).

Системные средства ОС Unix FreeBSD, позволяют построить довольно надежный межсетевой экран (систему защиты) и биллинговую систему. Входящая в ОС FreeBSD утилита ipfw является программным интерфейсом, позволяющим реализовать набора правил фильтрации, контролирующих весь IP-поток из удаленных систем в корпоративную сеть, и наоборот, – из корпоративной сети к удаленным системам. Функции ipfw-утилиты довольно разнообразны. Для решения поставленных задач важными являются следующие:

- запрет исходящих или приходящих IP-пакетов (защитные функции);
- подсчет пакетов и количества байт в пакете (функции учета);
- исследование IP-пакета по вышеуказанным параметрам (функции анализа).

Анализ IP-потока, моделирование систем защиты и биллинга на основе ОС Unix FreeBSD было проведено в сети EecNet (Центр Электроники и Схемотехники СПбГТУ). Эта сеть построена по двухуровневой схеме, внешний сегмент управляется ОС Unix FreeBSD, внутренний – ОС Windows NT.

В процессе работы были составлены правила прохождения IP-пакетов. Правила задавались в командной строке и в специальном конфигурационном файле (для воспроизведения набора правил после перезагрузки сервера).

Введение правил, включающих подсчет количественных характеристик потоков, позволил проанализировать трафик по портам некоторых Internet–служб, а именно: e-mail, FIDO, ICQ, Telnet, DNS, WEB, FTP.

Таким образом, подтвердилась идея, что брандмауэр, надежно защищающий данные корпоративной сети, может служить основой для построения эффективной системы анализа IP-потока и системы учета (биллинговой системы).

Использование только системных механизмов фильтрации позволяет:

- вести учет потребления Internet-ресурсов;
- выявлять паразитный трафик, который может свидетельствовать о попытках несанкционированного доступа к сети;
- построить правила доступа к Internet-ресурсам для корпоративной сети и проконтролировать их выполнение.

Сеть EecNet является прообразом двухуровневой корпоративной сети — она построена по архитектуре, способной поддерживать функционирование как совсем небольших, так и довольно крупных сетей, т.е. является масштабируемой в широких пределах. Это означает, что для подобных сетей, в том числе значительных размеров, биллинговые системы также можно строить на основе брандмауэров.