Математические структуры и моделирование
2004, вып. 13, с. 135–??

УДК 681.

СИСТЕМА КОНТРОЛЯ РАЗГРАНИЧЕНИЯ ДОСТУПА НА ОСНОВЕ ИССЛЕДОВАНИЯ КОРРЕЛЯЦИЙ ПОТОКОВ ДАННЫХ

В.И. Ефимов

In this article is presented new approach for traffic control

Сети передачи данных с коммутацией пакетов представляют собой систему промежуточных узлов (маршрутизаторы, прокси–устройства, сервера) соединенных между собой каналами передачи информации. Сеанс обмена информации в сети, представляет собой совокупность потоков проходящих через узлы сети. Эти потоки коррелированны и подчиняются определенным законам, например, ответ от dns–сервера может быть получен только после того, как был сгенерирован соответствующий запрос. В связи с этим, появляется дополнительный критерий проверки работы устройств на основе генерируемых этими устройствами потоков данных, что позволяет блокировать или разрешать взаимодействие между ними.

Рассмотрим систему, показанную на рис.1. ГП1, ГП2 – группы пользователей 1 и 2 принадлежащие различным сетям, Б – брандмауэр (межсетевой экран–маршрутизатор), Интернет – выход во внешнюю сеть.

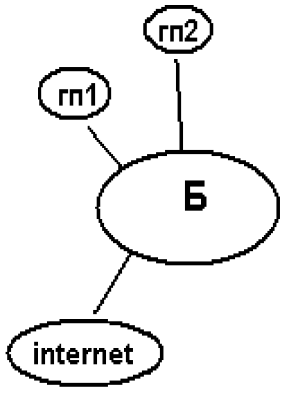

Рис. 1. Группы пользователей и брандмауэр

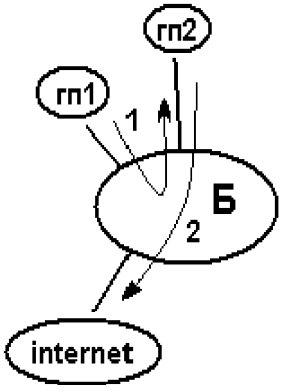

Рис. 2. Незаконный трафик

Омский государственный университет

Типичная задача, возникающая в данной ситуации, есть задача обеспечения контроля доступа. Рассмотрим следующие условия, наложенные на систему и методы реализации соответствующей концепции защиты.

Пусть ГП1 и ГП2 могут обмениваться данными между собой, ГП2 при этом имеет выход во внешнюю сеть (Интернет), пользователям ГП1 в соответствии с действующей политикой безопасности, доступ в Интернет блокирован.

Пусть Алиса находится в ГП1, а Боб, в ГП2. Алиса договорилась с Бобом, и Боб на своем компьютере установил программу «прокси–сервер». Алиса, подключается к программе «прокси–сервер» на компьютере Боба, и под видом Боба выходит в Интернет с его машины. Данная схема изображена на рис.2.

Номерами 1,2 показана последовательность прохождения исходящих данных с компьютера Алисы в сеть Интернет. Следует отметить, что 1 и 2 это разные tcp–соединения. С практической точки зрения, данная схема очень просто реализуется. Бобу достаточно поставить программу web–proxy (squid–например) на некоторый порт, а Алисе в настройках своего Веб–браузера, использовать в качестве прокси–сервера адрес машины Боба и порт. Предотвратить подобную ситуацию можно несколькими способами:

1. Самый простой способ – осуществлять пакетную фильтрацию между ГП1 и ГП2, разрешив прохождение только нужных для обмена информацией протоколов, т.е. запретить порты, на которые может быть поставленна «прокси–программа». Данное решение не всегда приемлимо, т.к, в современных сетях, нельзя ограничиться небольшим количеством портов, одна только служба распределенного каталога учетных записей пользователей ActiveDirectory в системе Windows использует порядка 10 портов, не говоря уже о том, что существует масса мультимедиа–приложений, вообще не привязанный к протоколу tcp или udp. Следовательно, Боб всегда найдет свободный открытый порт на своей машине, через который Алиса получит доступ к его «прокси–программе».

2. Более совершенным способом можно считать использование «контекстного» брандмауэра. Данный подход использует методы фильтрации трафика, но еще происходит и контроль протокола уровня приложений. Это помешает Бобу, на порт ftp–сервера например, установить свою «программу–прокси». В этом случае Алиса должна использовать конструкции протокола ftp между собой и Бобом (т.к. межсетевой экран ожидает видеть именно их), для доступа, например, к www–сайтам. Это достаточно сложная программа, но все же ее реализация не представляет особых трудностей, тем более, Боб сам может загружать определенные страницы по www из Интернет, сохранять их локально на своей машине, а Алиса забирать их позже по ftp. Также, брандмауэр не может «знать» все протоколы, разрешенные между Алисой и Бобом. Данные методы, основаны на способах фильтрации трафика.

3. Далее предлагается способ основанный на принципе контроля зависимостей между потоками данных.

Описываемая задача была смоделирована на оборудовании. На рис.3 показан трафик потоков 1 и 2.

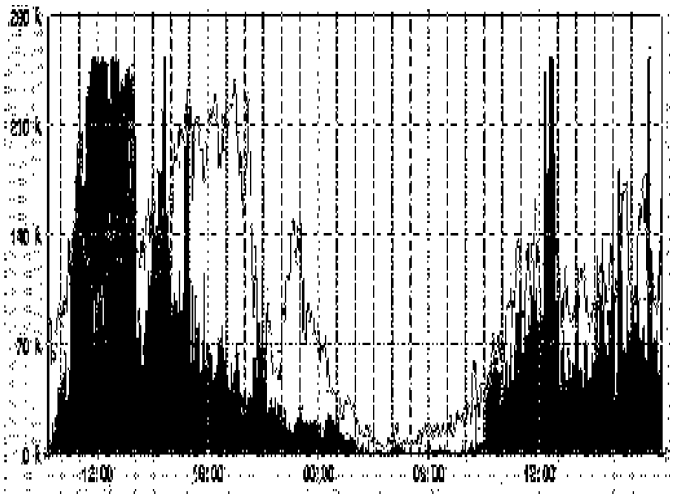

Рис. 3. Коррелированные трафики

Закрашенным показан трафик между ГП2 и Интернет, прозрачным, трафик между ГП1 и ГП2. Для анализа корреляционной зависимости этих потоков, была написана программа. Выборочный коэффициент корреляции вычислялся по формуле [1]:

$$r = \frac{n\sum\limits_{i=1}^{n} X_i Y_i - \sum\limits_{i=1}^{n} X_i \cdot \sum\limits_{i=1}^{n} Y_i}{\sqrt{\left[n\sum\limits_{i=1}^{n} X_i^2 - \left(\sum\limits_{i=1}^{n} X_i\right)^2\right]\left[n\sum\limits_{i=1}^{n} Y_i^2 - \left(\sum\limits_{i=1}^{n} Y_i\right)^2\right]}}$$

Величина коэффициента корреляции изменяется в интервале $-1 \leq 0 \leq 1$. При значении $r = 0$, корреляция между X и Y отсутствует, при $r = 1$, наблюдается полная корреляционная зависимость, при $r = -1$ существует обратная зависимость.

Следует отметить, что при частоте выборки 1 час (34 значения), коэффициент $r = 0.5$, при 30 минутной выборке (68 значений), полученный коэффициент $r = 0.7$. Анализ позволяет судить о коррелированности этих потоков.

Усилить проверку коррелированности потоков можно следующими способами.

а) Анализировать данные передаваемые по соединениям. То есть, если Боб из Интернет получил определенную строку символов, и далее эта строка передалась от Боба Алисе, скорее всего, что эти два потока взаимосвязаны.

б) Хронометрическую зависимость установления соединений. Если Алиса установив соединение с машиной Боба вызывает установление соединения машины Боба с серверами в Интернет, то эти соединения, вероятно, также зависимы.

Далее приводится алгоритм для проверки пакетов соединения на динамическом межсетевом экране.

Пусть существует Таблица A, представляющая собой одномерный список, время существования записи в котором t. Переменная штраф – соответствую-

щий критерий, на основе которого принимается решение о блокировке данных. Порог срабатывания для нее задается в переменной $\text{штраф}_{\text{макс}}$.

Каждый пакет, проходящий через брандмауэр, подвергается проверке, на основе которой, динамическим брандмауэром осуществляется соответствующее действие:

Проверка: Пакет от (ГП1) к (ГП2)?

Действие: Пропустить, занести запись о пакете в таблицу А.

Проверка: Пакет от (ГП2) к (Интернет)?

Действие:

Если запись в таблице А для пакета есть и штраф $<$ $\text{штраф}_{\text{макс}}$,
то штраф увеличить на 1, пакет пропустить;
Если записи в таблице А нет и штраф $<$ $\text{штраф}_{\text{макс}}$,
то штраф уменьшить на 1, пакет пропустить;
Если штраф $\geq$ $\text{штраф}_{\text{макс}}$,
то пакет блокировать.

Данные, заносимые в таблицу, однозначно идентифицирующие пакет, есть сетевые адреса отправителя, получателя, и номера их портов.

В данном случае, варьируя параметрами, время сохранения записи в таблицы и $\text{штраф}_{\text{макс}}$, можно анализировать зависимости потоков (ГП1–ГП2) и (ГП2–Интернет) и управлять трафиком.

4. На основе принудительного вмешательства со стороны брандмауэра. Если брандмауэр принудительно уменьшит полосу пропускания на одном из потоков, это, при некоторых условиях, должно отразиться и на зависимом потоке.

Рассмотрим последний способ подробнее. Пусть Боб поставил программу «прокси–сервер» на порт своего компьютера. Алиса установила tcp–соединение с компьютером Боба, а компьютер Боба установил соединение с сервером в Интернет. При этом, машина Боба, имеет соединение с Интернет со скоростью 56k, а Алиса использует для связи с Бобом, скоростную среду 100M. Рис.4 наглядно представляет эту схему.

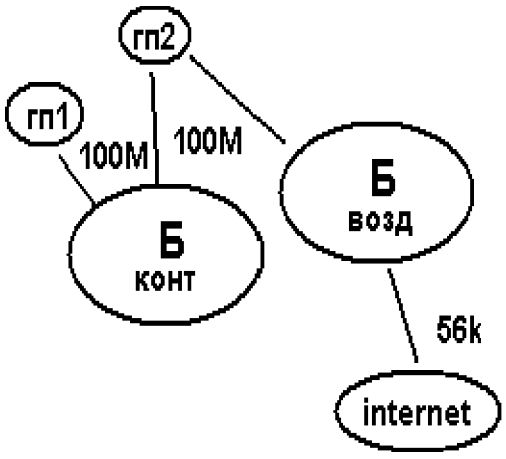

Рис. 4. Принудительное вмешательство брандмауэра

Физически, брандмауэр Б представляет одно устройство. Логически его можно разделить на «брандмауэр воздействия» и «брандмауэр контроля», поскольку трафик проходит через него два раза. Пусть «брандмауэр воздействия», удалит пакет из соединения ГП2 (Боба) с Интернетом. Машина Боба будет ожидать получение данного пакета от сервера в Интернете. После того, как сервер не получит подтверждения на переданный Бобу пакет, он сделает попытку послать его повторно. За это время, поток данных между ГП2 и ГП1, также приостановится, что будет обнаружено «брандмауэром контроля», и будет наложен запрет на передачу трафика с машины Алисы и порта прокси на машине Боба. Если же скорость канала между Бобом и Алисой будет меньше чем скорость канала между Бобом и сервером в Интернет, то задержки может не быть, поскольку в буфере обмена на машине Боба в соединении между Бобом и Алисой будут данные, которые по-прежнему будут передаваться.

Последний метод сочетает в себе совокупность двух принципов: динамическую фильтрацию плюс динамическое слежение за качеством обслуживания в сети.

Развитием метода контроля трафика на основе коррелированных потоков, может быть разработка систем нового поколения интеллектуальных устройств контроля прохождения трафика в сети, где брандмауэр обучается логике работы сети на основе транзакций происходящих в ней.

Литература

1. Колемаев В.А., Староверов О.В., Турундаевский В.Б. *Теория вероятностей и математическая сатистика.* М.: Наука. 1991.