МЕХАНИЗМЫ ЗАЩИТЫ КОРПОРАТИВНЫХ СЕТЕЙ

Володин С.А., группа ТКС-06мн
Руководитель проф. каф. АТ Хорхордин А.В.

Интенсивное развитие глобальных компьютерных сетей и появление новых технологий поиска информации привлекают все больше внимания к сети Internet со стороны частных лиц и различных организаций. Многие организации принимают решение об интеграции своих локальных и корпоративных сетей в глобальную сеть. Использование глобальных сетей в коммерческих целях, а также при передаче по сетям информации, содержащей сведения конфиденциального характера, влечет за собой необходимость построения эффективной системы защиты информации.

С целью избежания несанкционированного доступа к своим сетям многие компании, подключенные к Internet, полагаются на брандмауэры. Однако, достигая при этом своей основной цели, пользователь брандмауэра сталкивается с необходимостью выбора между удобством работы и безопасностью системы. Существует множество вариантов обеспечения защиты корпоративных сетей, но, в принципе, брандмауэр можно представить как пару механизмов: один — для блокировки, второй — для разрешения трафика.

Основной причиной для установки в частной сети брандмауэра практически всегда является стремление пользователя защитить сеть от несанкционированного вторжения. В большинстве случаев сеть защищают от нелегального доступа к системным ресурсам, а также от отправки какой либо информации вовне баз ведома её владельца.

Существует несколько путей свести на нет либо обойти брандмауэрную защиту. И хотя они все могут создать проблемы, о некоторых можно с уверенностью говорить как о самых неприятных. Исходя из того, что основной целью установки большинства брандмауэров является блокирование доступа, очевидно, что

обнаружение кем-либо лазейки, позволяющей проникнуть в систему, ведет к полному краху всей защиты данной системы. Если же несанкционированному пользователю удалось проникнуть в брандмауэр и переконфигурировать его, ситуация может принять еще более угрожающий характер. В целях разграничения терминологии можно принять, что в первом случае мы имеют дело со взломом брандмауэрной защиты, а во втором — с полным ее разрушением. Степень ущерба, который может повлечь за собой разрушение брандмауэрной защиты, определить невероятно сложно.

Но, несмотря на эффективность в целом, брандмауэр не обеспечивает защиту от собственного персонала или от злоумышленника, уже преодолевшего это средство сетевой защиты. Для решения задач по отражению наиболее вероятных угроз для внутренних сетей рационально использовать в дополнение межсетевые экраны (МЭ). В арсенале ИТ-профессионалов межсетевые экраны остаются главным оружием для борьбы со взломщиками. Межсетевой экран позволяет разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet, хотя ее можно провести и внутри корпоративной сети предприятия. МЭ пропускает через себя весь трафик, принимая для каждого проходящего пакета решение — пропускать его или отбросить. Для того чтобы МЭ мог это осуществить, ему необходимо определить набор правил фильтрации.

Ни один межсетевой экран не может гарантировать полной защиты внутренней сети при всех возможных обстоятельствах. Однако, для большинства коммерческих организаций установка межсетевого экрана является необходимым условием обеспечения безопасности внутренней сети. Главный довод в пользу применения межсетевого экрана состоит в том, что без него системы внутренней сети подвергаются опасности со стороны слабо защищенных служб сети Internet, а также зондированию и атакам с каких-либо других хост-компьютеров внешней сети.

Межсетевые экраны можно разделить на четыре основные категории: МЭ с высоким коэффициентом готовности, защищающие периметр сети; collocated МЭ, предназначенные для обслуживания многочисленных клиентов сервис-провайдеров (xSP); МЭ для SOHO, разворачиваемые и администрируемые сервис-провайдерами и персональные межсетевые экраны, которые управляются централизованно и предназначены для корпоративных настольных систем [1].

У каждого МЭ есть свои преимущества и недостатки. И этим обуславливается то, что при выборе технологии главный упор должен быть сделан на требованиях приложения, а не чем-то другом.

Эффективность защиты внутренней сети с помощью межсетевых экранов зависит не только от выбранной политики доступа к сетевым сервисам и ресурсам внутренней сети, но и от рациональности выбора и использования основных компонентов межсетевого экрана.

Функциональные требования к межсетевым экранам включают:

- требования к фильтрации на сетевом уровне;
- требования к фильтрации на прикладном уровне;
- требования по настройке правил фильтрации и администрированию;
- требования к средствам сетевой аутентификации;
- требования по внедрению журналов и учету.

Большинство компонентов межсетевых экранов можно отнести к одной из трех категорий:

- фильтрующие маршрутизаторы;
- шлюзы сетевого уровня;
- шлюзы прикладного уровня.

Эти категории можно рассматривать как базовые компоненты реальных межсетевых экранов. Лишь немногие межсетевые экраны включают только одну из перечисленных категорий. Тем не менее, эти категории отражают ключевые возможности, отличающие межсетевые экраны друг от друга [2].

На сегодняшний день лучшей защитой от компьютерных преступников является межсетевой экран правильно установленный и подобранный для каждой сети. Необходимость создания минимально уязвимых корпоративных сетей обуславливает актуальность разработки наиболее эффективных средств информационной безопасности. Этой теме посвящена магистерская работа на кафедре автоматики и телекоммуникаций. Задачей данного исследования является изучение требований по безопасности сети предприятия и разработка комплексного решения по обеспечению защиты информационной сети с использованием программно-аппаратных средств предотвращения вторжений.

Перечень ссылок

1. Сети и системы связи №2 (80) 1 марта 2002 — 83 с.

2. Защита информации в компьютерных системах и сетях/ Под ред. В.Ф. Шаньгина.— М.: Радио и связь, 1999.—328 с.