УДК 621.3

МЕЖСЕТЕВЫЕ ЭКРАНЫ КАК МЕРА ЗАЩИТЫ ОТ КИБЕРАТАК

Федосевич Э.А.

Научный руководитель – Сапожникова А.Г.

Одним из самых популярных методов защиты локальной сети от кибератак извне является использование межсетевого экрана (МСЭ). Межсетевой экран (firewall, брандмауэр) представляет собой программную или программно-аппаратную систему, которая устанавливается на границе охраняемой вычислительной сети и осуществляет фильтрацию сетевого трафика в обе стороны, разрешая или запрещая прохождение определенных пакетов внутрь локальной сети (в периметр безопасности) или из нее в зависимости от выбранной политики безопасности. Однако, только фильтрацией пакетов задачи современных МСЭ не ограничиваются, они выполняют также множество дополнительных действий:

– кэширование информации, когда часть полученной из внешней сети информации временно сохраняется на локальных запоминающих устройствах, что позволяет экономить время и потребляемый трафик при повторном обращении к той же информации;

– трансляция адресов, позволяющая использовать для внешних коммуникаций компьютеров локальной сети только один IP-адрес – адрес самого брандмауэра, внутренние адреса локальной сети могут быть любыми;

– переадресация, позволяющая отправлять пакеты, приходящие на некоторый IP-адрес, на компьютер с другим адресом. Это позволяет, например, распределить нагрузку на Web-сервер.

Существуют два основных типа МСЭ: пакетные фильтры и шлюзы приложений. При этом оба типа могут быть реализованы одновременно в одном брандмауэре. Пакетные фильтры (packet filter) представляют собой сетевые маршрутизаторы, которые принимают решение о том, пропускать или блокировать пакет на основании информации в его заголовке (рисунок 1).

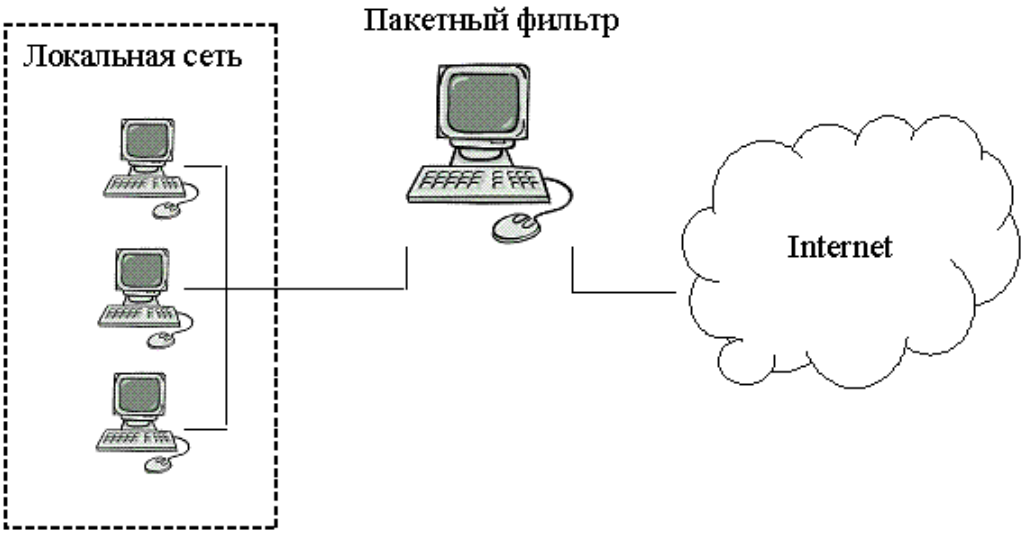

Рисунок 1. Пакетный фильтр на границе локальной сети

Пакетные фильтры работают с информацией в заголовках IP, ICMP, TCP и UDP – пакетов. Правила фильтрации пакетов задаются на основе следующих данных:

– название сетевого интерфейса и направление передачи информации;
– IP-адреса отправителя и получателя;
– протокол более высокого уровня (используется TCP или UDP);
– порт отправителя и получателя для протоколов TCP и UDP;
– опции IP (например, блокировка маршрутизации от источника);
– тип сообщения ICMP.

При определении правил фильтрации необходимо придерживаться одной из двух стратегий политики безопасности:

1. Разрешить весь трафик, не запрещенный правилами фильтрации.
2. Запретить весь трафик, не разрешенный правилами фильтрации.

С точки зрения безопасности более предпочтительной является вторая стратегия, согласно которой задаются правила, разрешающие прохождение пакетов определенного типа, прохождение остальных пакетов запрещается. Это связано с тем, что, во-первых, количество запрещенных пакетов обычно гораздо больше, чем количество разрешенных, а во-вторых, со временем могут появиться новые службы, для которых при использовании первой стратегии необходимо будет дописывать запрещающие правила (если доступ к ним, конечно, нежелателен), в то время как вторая стратегия запретит доступ к ним автоматически.

Пакетные фильтры классифицируются на фильтры без памяти и фильтры с памятью (динамические). Первые из них фильтруют информацию только исходя из информации в заголовке рассматриваемого пакета. Динамические же пакеты учитывают при фильтрации текущее состояние соединений, формируя таблицы входящих и исходящих пакетов, и принимают решение на основании информации в нескольких взаимосвязанных пакетах.

Кроме того, пакетные фильтры могут реализовывать также множество дополнительных возможностей. Например, перенаправление пакетов, дублирование пакетов, подсчет трафика, ограничение полосы пропускания, запись пакетов в файл протокола и многое другое. Настройка пакетного фильтра требует от администратора значительной квалификации и понимания принципов работы всех протоколов стека TCP/IP от протоколов прикладного уровня до протоколов сетевого уровня.

Большинство современных операционных систем имеют встроенные пакетные фильтры, например, ipfw в Unix или Internet Connection Firewall в Windows. Функции пакетного фильтра могут выполнять и аппаратные маршрутизаторы, например, CISCO PIX 515E.

Главным недостатком пакетных фильтров является невозможность осуществления фильтрации пакетов по содержимому информационной части пакетов, то есть по данным, относящимся к пакетам более высокого уровня. Этот недостаток может быть устранен путем использования шлюзов приложений (application gateway, proxy-server). Proxy-серверы работают на прикладном уровне, обеспечивая работу той или иной сетевой службы. При этом в отличие от пакетных фильтров, которые лишь перенаправляют пакет из одной сети в другую, proxy-серверы принимают запрос от клиента и направляют его во внешнюю сеть от своего имени, разрывая таким образом нормальный сетевой трафик (рисунок 2). Поэтому брандмауэр в виде шлюза приложений может быть реализован на компьютере всего с одним сетевым интерфейсом.

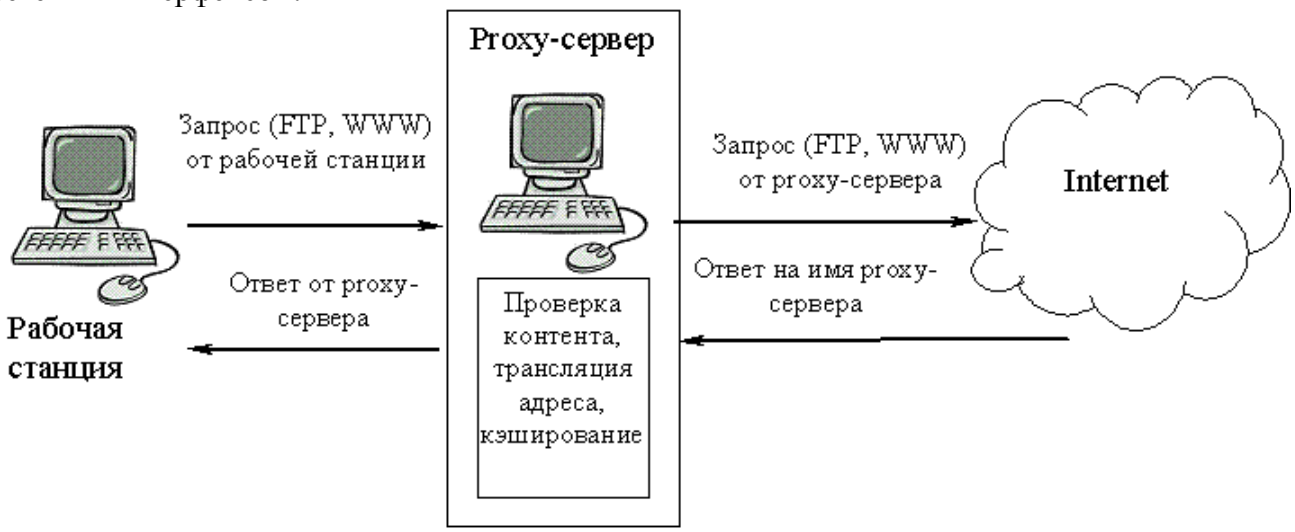

Рисунок 2. Выполнение запроса через proxy-сервер

Поясним схему на рисунке 2. Клиент формирует запрос на сервер какой-либо службы в Internet (например, запрос на внешний Web-сервер). Запрос поступает на proxy-сервер (конфигурация брандмауэра должна быть такова, чтобы все запросы к какой-либо службе в Internet обязательно поступали на соответствующий proxy-сервер). Приняв запрос от клиента, proxy-сервер проверяет его по заданным правилам фильтрации содержимого пакета и, если запрос не содержит запрещенных параметров, формирует пакет с запросом уже от своего имени (со своим обратным адресом) внешнему серверу. Ответ от внешнего сервера поступает, очевидно, на имя proxy-сервера. Пройдя проверку, аналогичную запросу, ответ может быть принят либо отвергнут. Если ответ принят – ответ направляется на адрес клиента, первоначально сформировавшего запрос.

Фильтрация содержимого может осуществляться по множеству параметров:

– IP-адрес отправителя и получателя;

– запрашиваемый URL;

– наличие вложений (приложения Java, компоненты ActiveX) и т. п.

– время запроса и другие, в зависимости от используемого proxy-сервера.

Важной функцией современных proxy-серверов является трансляция сетевых адресов (Network Address Translation, NAT), которая подразумевает замену адреса клиента в запросе во внешнюю сеть на собственный адрес (или несколько адресов) proxy-сервера. Это позволяет скрыть от посторонних структуру внутренней сети, список используемых в ней адресов. С другой стороны, это позволяет иметь на всю локальную сеть лишь один легальный IP-адрес, который должен быть присвоен proxy-серверу. Рабочие станции внутри сети могут иметь любые IP-адреса, в том числе и те, которые запрещено использовать во внешней сети. NAT может быть организована по статической и динамической схеме. При статической трансляции адрес клиента в локальной сети привязывается к конкретному адресу, который транслируется во внешнюю сеть. Динамическая трансляция предполагает наличие диапазона доступных внешних адресов и при каждом запросе клиента proxy-сервер выделяет один из свободных адресов для представления клиента во внешней сети, по окончании транзакции этот адрес возвращается в список свободных и может быть использован в дальнейшем для передачи запроса другого клиента. Развитием идеи NAT стала трансляция адресов портов (Network Address Port Translation, NAPT), когда один и тот же IP-адрес распределяется при трансляции на несколько пользователей и каждому пользователю сопоставляется в отправляемом во внешнюю сеть пакете уникальная комбинация IP-адреса и номера порта отправителя. Иными словами, различным пользователям сети proxy-сервер сопоставляет один и тот же IP-адрес, но присваивает различные номера портов в исходящих запросах. Это стало возможным за счет того, что порт отправителя зачастую не несет в запросе никакой полезной информации и может быть использован для уникальной идентификации клиента локальной сети для proxy-сервера.

Современные proxy-серверы выполняют обычно еще одну важную функцию – кэширование информации. Информация, пришедшая на proxy-сервер, сохраняется на локальных запоминающих устройствах, и при очередном запросе клиента запрашиваемая им информация сначала ищется в локальной памяти, и только если ее там нет – запрос передается во внешнюю сеть. Это позволяет уменьшить объем трафика, потребляемого из внешней сети, а также уменьшить время доступа к информации для конечного клиента.

Рассмотрим свойства наиболее распространенных proxy-серверов.

Microsoft Proxy Server (версия 2.0) представляет собой брандмауэр с расширяемым набором функций и сервер кэширования информации, обеспечивает поддержку протоколов HTTP и gopher, а также поддержку клиентских приложений (например, Telnet и RealAudio) для компьютеров интрасети, использующих протоколы TCP/IP или IPX/SPX, поддерживает VPN, выполняет функции фильтра пакетов. Работает в среде Windows.

Squid – высокопроизводительный кэширующий proxy-сервер для web-клиентов с поддержкой протоколов FTP, gopher и HTTP, имеющий реализации как под Unix, так и под Windows – платформы.Squid хранит метаданные и особенно часто запрашиваемые объекты в

ОЗУ, кэширует DNS-запросы, поддерживает неблокирующие DNS-запросы и реализует негативное кэширование неудачных запросов. Поддерживает протокол ICP (Internet Casing Protocol), позволяющий организовывать нескольким серверам иерархические структуры кэширования.

Помимо перечисленных, на практике могут быть использованы так называемые персональные межсетевые экраны. Они устанавливаются на компьютер пользователя, и все правила безопасности задаются для обмена этого компьютера с внешней сетью. Это позволяет настроить политику безопасности персонально под каждого пользователя непосредственно на его рабочей станции. Примером подобного МСЭ является брандмауэр AtGuard, который включает в себя функции proxy-сервера и локального пакетного фильтра. AtGuard способен блокировать баннеры, файлы cookie, Java-скрипты и апплеты, а также элементы ActiveX. Еще одна особенность AtGuard – способность работать в режиме обучения, когда при каждой попытке подключиться к какому-либо порту запрашивается разрешение на установку соединения, и сделанный пользователем выбор становится правилом для дальнейшей работы программы.

Литература

1. Лапонина, О.Р. Межсетевые экраны / О.Р. Лапонина. – М. : ИНТУИТ, 2016. – 466 с.

2. Лебедь, С.В. Межсетевое экраничование. Теория и практика защиты внешнего периметра / С.В. Лебедь. – М. : МГТУ им. Н.Э. Баумана, 2002. – 306 с.

3. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере / А.Е. Форонов. – М. : ИНУИТ, 2016. – 155 с.