УДК 004.056.5

ИСПОЛЬЗОВАНИЕМ МЕЖСЕТЕВЫХ ЭКРАНОВ В МОНИТОРИНГЕ БЕЗОПАСНОСТИ ДОВЕРИТЕЛЬНОЙ СРЕДЫ ЛВС

***В.А. Клаченков**, аспирант БГУИР*
*Научный руководитель – **Д.И. Руско***
Полесский государственный университет

Быстрый темп развития информационных систем в современных условиях невозможно без обеспечения соответствующей информационной безопасности. Обеспечение информационной безопасности требует комплексного и целостного подхода, при этом особого внимания требуют вопросы обеспечения безопасности информации при ее обработке в автоматизированных системах: автономно работающих компьютерах и локальных сетях. Для обеспечения безопасности, необходимо, в первую очередь определить механизмы, которые защищают информацию и информационные системы, гарантируют доступность, целостность, аутентификацию, конфиденциальность и невозможность отказа [1].

На сегодняшний день одним из самых популярных методов защиты ЛВС от внешних атак является использование межсетевого экрана. Межсетевой экран – программно-аппаратная система межсетевой защиты, которая отделяет один сегмент локальной вычислительной сети от другого и реализует набор правил для прохождения данных из одного сегмента в другой. Границей является раздел между корпоративной локальной сетью и внешними Internet-сетями или различными сегментами локальной распределенной сети. Экран фильтрует текущий трафик, пропуская одни пакеты информации и отсеивая другие.

Среди функций, которые выполняют межсетевые экраны основными являются настройка правил фильтрации, администрирование доступа во внутренние сети, фильтрацию на сетевом уровне, фильтрацию на прикладном уровне, средства сетевой аутентификации, ведение журналов и учет.

Анализ литературных данных за последнее десятилетие показал, что в настоящее время успешно используются два основных типа межсетевых экранов: пакетные фильтры, и шлюзы приложений.

Пакетные фильтры представляют собой сетевые маршрутизаторы, которые принимают решение о том, пропускать или блокировать пакет на основании информации в его заголовке и работают с информацией в заголовках IP, ICMP, TCP и UDP- пакетов. Распространенность использования фильтров пакетов обусловлена возможностью создавать гибкие схемы разграничения доступа на основе специального набора правил с задаваемыми параметрами:

- 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;
- 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.

При этом наиболее предпочтительно использование второй стратегии. Это связано с тем, что количество запрещенных пакетов гораздо больше, чем разрешенных, а в будущем могут появиться новые службы, для которых, если использовать первую стратегию необходимо будет дописывать запрещающие правила, в то время как вторая стратегия запретит доступ к ним автоматически.

Классификация пакетных фильтров:

фильтры без памяти;

фильтры с памятью.

Первые фильтруют информацию только исходя из информации в заголовке рассматриваемого пакета. Вторые учитывают текущее состояние соединений, формируя таблицы входящих и исходящих пакетов, и принимают решение на основании информации в нескольких взаимосвязанных пакетах.

Основным недостатком пакетных фильтров является невозможность осуществления фильтрации пакетов по содержимому информационной части, то есть по данным, относящимся к пакетам более высокого уровня. Этот недостаток устраняется путем использования шлюзов приложений, которые функционируют на прикладном уровне, обеспечивая работу той или иной сетевой службы .

К числу широко используемых прокси серверов относятся:

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, использующих протоколы TCP/IP или IPX/SPX, поддерживает VPN, выполняет функции фильтра пакетов.

Squid - высокопроизводительный кэширующий прокси-сервер для web-клиентов с поддержкой протоколов FTP, gopher и HTTP, имеющий кроссплатформенную реализацию, хранит метаданные и часто запрашиваемые объекты в ОЗУ, поддерживает неблокирующие DNS-запросы, кэширует DNS-запросы и реализует негативное кэширование неудачных запросов. Поддерживает протокол ICP, позволяющий организовывать нескольким серверам иерархические структуры кэширования.

Для обеспечения комплексной безопасности на практике используются межсетевые экраны, представляющие собой интегрированную систему защиты, включающую как пакетный фильтр, так и прокси-сервер. Они могут располагаться на одном либо нескольких компьютерах, в связи с чем существует возможность выбора архитектуры используемого межсетевого экрана. Выбор конкретной архитектуры межсетевого экрана зависит от стоящих перед администратором задач, условий функционирования, стоимости того или иного решения [2].

Архитектура с использованием в качестве межсетевого экрана компьютера с двумя сетевыми интерфейсами похожа на схему подключения пакетного фильтра, но на самом межсетевом экране должна быть отключена возможность маршрутизации пакетов. Это позволяет полностью блокировать трафик во внешнюю сеть на этом компьютере, а все необходимые сервисы должны обеспечиваться прокси-серверами, работающими на двухканальном компьютере. Для обеспечения дополнительной защиты можно поместить маршрутизатор с фильтрацией пакетов между внешней сетью и двухканальным компьютером.

Архитектура с экранированным узлом предполагает одновременное использование пакетного фильтра и прокси-сервера. На границе с внешней сетью устанавливается пакетный фильтр, который должен блокировать потенциально опасные пакеты, чтобы они не достигли прикладного шлюза и локальной сети. Он отвергает или пропускает трафик в соответствии со следующими правилами:

- трафик из внешней сети к прикладному шлюзу пропускается;
- прочий трафик из внешней сети блокируется;
- пакетный фильтр блокирует любой трафик из локальной сети во внешнюю, если он не идет от прикладного шлюза.

Прикладной шлюз должен обеспечивать функции прокси-сервера для всех потенциально опасных служб и для нормального функционирования достаточно одного сетевого интерфейса.

Подобная схема подключения брандмауэра отличается большей гибкостью по сравнению с двухканальным межсетевым экраном, поскольку пакетный фильтр может позволить пропустить запросы к надежным сервисам в обход прикладного шлюза. Этими надежными сервисами могут быть те сервисы, для которых нет прокси-сервера, и которым можно доверять в том смысле, что риск использования этих сервисов считается приемлемым.

Таким образом, неотъемлемой частью сетевой безопасности является использование межсетевых экранов, которые способствуют предотвращению внешних атак, возникающих при передаче информации по сетям. Однако применение только лишь межсетевых экранов является недостаточным для обеспечения информационной безопасности, в связи с чем изучение дополнительных средств безопасности и связанных с ними теоретических и прикладных проблем является актуальной задачей, требующей более глубокого изучения.

Список использованных источников

1. Ясенев, В.Н. Информационная безопасность: учебное пособие / В.Н. Ясенев, А.В. Дорожкин, А.Л. Сочков. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с.

2. Оглтри, Т. Практическое применение межсетевых экранов / Оглтри Т. – М.: ДМК Пресс, 2001. – 400 с.