УДК 004.056
DOI 10.21685/2587-7704-2020-5-2-8

Open Access RESEARCH ARTICLE

Применение межсетевых экранов в сети в соответствии с установленными нормативными документами Федеральной службы по техническому и экспертному контролю

Л. И. Трофимова
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Произведено описание работы межсетевых экранов. Определены виды межсетевых экранов. Проанализированы классы защищенности межсетевых экранов. Определена возможность применения межсетевого экрана в соответствии с требованиями, установленными Федеральной службой по техническому и экспертному контролю.

Ключевые слова: межсетевой экран, информация, классы защищенности, фильтрация, сеть.

Application of network firewalls in accordance with the established regulations of the Federal Service for Technical and Export Control

L. I. Trofimova
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The article describes the operation of firewalls. The types of firewalls are defined, and their security classes are analyzed. The possibility of using a firewall in accordance with the requirements established by the Federal Service for Technical and Export Control has been determined.

Keywords: firewall, information, security classes, filtering, network.

В современном мире существуют различные виды защиты информации от разнообразных внешних и внутренних воздействий. Одним из таких является межсетевой экран.

Межсетевой экран является программной или программно-аппаратной частью сети, которая осуществляет фильтрацию и контроль данных, проходящих через него.

Более подробное описание дает ГОСТ Р ИСО/МЭК 27033-1-2011 [1]. Межсетевой экран выступает как вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую, и, наоборот, при этом пропускается только авторизованный трафик, соответствующий местной политике безопасности [1].

Из данного определения можно выделить несколько основных угроз, риск исполнениях которых может уменьшить межсетевой экран:

– несанкционированный доступ к защищаемой информации;

– отказ в обслуживании узлов, устройств из-за неуправляемых сетевых подключений;

– внедрение вредоносного кода в передаваемые данные.

На основании приведенных угроз будут различаться и виды межсетевых экранов. Функционирование межсетевых экранов возможно на разных уровнях сети. Так как они взаимодействуют с сетью, то они будут классифицироваться на основании уровней модели OSI. Условно можно выделить несколько видов по уровням:

– управляемые коммутаторы – канальный уровень;
– сетевые фильтры – сетевой уровень;
– шлюзы сеансового уровня;
– посредники прикладного уровня;
– инспекторы состояния – сеансовый уровень.

Данная классификация может быть не совсем точной, так как межсетевые экраны могут функционировать на нескольких уровнях модели OSI. Поэтому применимость межсетевых экранов может быть не конкретизирована.

Для дальнейшей применимости межсетевых экранов Федеральная служба по техническому и экспертному контролю (ФСТЭК) в информационном сообщении «Об утверждении требований к межсетевым экранам» от 28 апреля 2016 г. № 240/24/1986 [2] определяет следующие виды межсетевых экранов:

– межсетевой экран уровня сети;
– межсетевой экран уровня логических границ сети;
– межсетевой экран уровня узла;
– межсетевой экран уровня веб-сервера;
– межсетевой экран уровня промышленной сети.

Межсетевой экран уровня сети применяется на физической границе [2] сети или системы или на границе сегментов сети или системы. Так как такие межсетевые экраны физически устанавливаются в сети, то их реализация возможна только программно-технически.

Межсетевой экран уровня логических границ сети [2] устанавливается на логической границе сети или на логической границе сегментов сети. Такие межсетевые экраны находятся на логической границе, поэтому они могут иметь программную или программно-техническую реализацию.

Межсетевой экран уровня узла [2] используется на узле сети или системы. Такой тип может иметь только программную реализацию при условии, что будет установлен на мобильных или стационарных [2] технических средствах.

Межсетевой экран уровня веб-сервера [2] может использоваться как на физической границе сегмента, так и непосредственно на серверах сайтов, служб и приложений. Они применяют программную и программно-техническую реализацию.

Межсетевой экран уровня промышленной сети [2] применяется в автоматизированной системе управления технологическими или производственными процессами [2]. Такие межсетевые экраны могут иметь программную или программно-техническую реализацию.

Использование межсетевых экранов происходит в разных сферах. Они имеют широкую применимость, так как везде необходим контроль и фильтрация информации. Но информация бывает ограниченного доступа, и в этом случае использование межсетевых экранов общего доступа неприемлемо. Поэтому для межсетевых экранов существуют свои классы защищенности. На основании документа «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [3] выделяются пять классов защищенности.

Первый класс защищенности самый высокий. Межсетевой экран должен обеспечивать фильтрацию на сетевом, транспортном уровне. Должен учитываться сетевой интерфейс входа и выхода, а также учитываются значимые поля сетевых пакетов. Используется идентификация и аутентификация при запросах над доступ. По необходимости используются биометрические характеристики или специальные устройства.

Межсетевые экраны первого класса используют средства контроля целостности с помощью контрольных сумм. Также поддерживаются следующие требования:

– восстановление оборудования;
– тестирование внутренних процессов;
– регистрация фильтруемых пакетов;
– уведомление о нарушении правил фильтрации;
– регистрация запусков программ;
– возможность единого управления компонентов.

– простота использования.

Второй и третий классы защищенности используют такие же требования, как и первый. Но они не могут обеспечивать идентификацию и аутентификацию всех субъектов прикладного уровня [3], и не предоставляется аутентификация и идентификация специальными устройствами или биометрическими характеристиками. Также межсетевой экран второго и третьего класса защищенности не может обеспечивать возможность единого управления компонентов.

Отличие третьего от второго класса в том, что в третьем классе нет уведомления о попытках нарушений правил фильтрации и уведомлений на события в межсетевом экране. Не осуществляется регистрация и учет сервисов, а также идентификация и аутентификация субъектов прикладного уровня [3].

Четвертый и пятый класс защищенности являются наиболее низкими. В данных классах используются те же требования, что и в предыдущих, за исключением некоторых показателей. Они не обеспечивают идентификацию и аутентификацию запросов входящих и исходящих. Также не обеспечивается возможность дистанционного управления частей межсетевого экрана.

Пятый класс защищенности является самым низким классом, его главным отличием от четвертого является отсутствие регистрации и учета обрабатываемых пакетов.

На основании различных типов межсетевых экранов и их разделения на классы защищенности можно сделать вывод о том, что они имеют широкое применение в сфере защиты информации. Но несмотря на все функции, которые могут реализовываться в межсетевых экранах по приведенным требованиям, возможно выделить некоторые недостатки.

Одним из недостатков можно назвать невозможность защиты от авторизированных пользователей. Запрет для незарегистрированных пользователей выполняется, но самим пользователям ограничить доступ нельзя. Поэтому пользователи являются внутренними нарушителями. Устранить данный недостаток возможно при помощи дополнительных систем.

Еще одним минусом является отсутствие поддержки защиты новых сетевых протоколов. Межсетевые экраны обеспечивают защиту по самым распространенным протоколам, например HTTP, SMTP и др. Для новых протоколов защита будет отсутствовать.

Межсетевые экраны, как правило, не имеют защиты от вирусов и атак. Это также можно отнести к минусам использования межсетевых экранов. Но данный минус можно устранить с использованием вспомогательных модулей и программ.

К недостатку можно отнести отсутствие контроля собственной конфигурации. Межсетевой экран, как правило, обеспечивает защиту корпоративных ресурсов, но не защиту внутренних настроек. По истечении времени первичная настройка устройства изменяется, что приводит к образованию большого количества правил. Возможна ситуация, когда некоторые ограничения будут не работать.

Несмотря на все недостатки при использовании межсетевых экранов, они имеют широкое применение. Они обеспечивают обширный функционал для реализации фильтрации и контроля обрабатываемой информации. Для работы с информацией разного рода межсетевые экраны также имеют несколько классов защиты, что позволяет им расширить область применения.

Библиографический список

1. ГОСТ Р ИСО/МЭК 27033-1–2011. – URL: http://docs.cntd.ru/document/gost-r-iso-mek-27033-1-2011 (дата обращения: 29.10.2020).
2. Информационное сообщение об утверждении требований к межсетевым экранам от 28 апреля 2016 г. № 240/24/1986 – URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1142-informatsionnoe-soobshchenie-fstek-rossii-ot-28-aprelya-2016-g-n-240-24-1986 (дата обращения: 30.10.2020).
3. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации : [утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.]. – URL: https://fstec.ru/component/attachments/download/295 (дата обращения: 01.11.2020).

Образец цитирования:

Трофимова, Л. И. Применение межсетевых экранов в сети в соответствии с установленными нормативными документами Федеральной службы по техническому и экспертному контролю / Л. И. Трофимова // Инжиниринг и технологии. – 2020. – Vol. 5(2). – С. 1–3. – DOI 10.21685/2587-7704-2020-5-2-8.