УДК 004.4
DOI 10.21685/2587-7704-2019-4-1-3

Open Access | RESEARCH ARTICLE

Проект модуля межсетевого экрана в составе устройства – маршрутизатора сетевых пакетов

В. А. Власова
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

В. Б. Варламов
Пензенский научно-исследовательский электротехнический институт,
Россия, 440000 г. Пенза, ул. Советская, 9

Аннотация. Проведен обзор типов межсетевых экранов. Выявлены достоинства и недостатки типов межсетевых экранов.

Ключевые слова: межсетевой экран, фильтрация, трафик, пакетный фильтр, прокси-сервер, контроль состояния, маршрутизатор, модель OSI.

Firewall module project as a part of network packet router

V. A. Vlasova
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

V. B. Varlamov
Penza Research Institute of Electrical Engineering, 9 Sovetskaya Street, 440000, Penza, Russia

Abstract. A review of firewall types was conducted. Advantages and disadvantages of firewalls are revealed.

Keywords: firewall, filtering, traffic, packet filter, proxy server, state control, router, OSI model.

В последнее время тема использования межсетевых экранов становится актуальной, потому что все большее число людей и организаций оказываются жертвами компьютерных взломщиков. И тем не менее количество пользователей в сети не уменьшается, а, наоборот, растет с огромной прогрессией.

Согласно [1], межсетевой экран (МСЭ) – это локальное (однокомпонентное) или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и (или) выходящей из АС. МСЭ обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя, таким образом, разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

Для построения межсетевого экрана используется определенный метод проверки пакета. В каждом методе используется информация от различных уровней модели взаимосвязи открытых систем. Известные три типа межсетевых экранов:

– пакетные фильтры;
– межсетевые экраны с контролем состояния;
– прокси-серверы.

Пакетные фильтры – самый простой метод проверки пакета. Процесс фильтрования пакета заключается в исследовании информации, содержащейся в заголовке, и сравнении ее с предварительно сконфигурированной группой правил или фильтрами. Каждый пакет может исследоваться индивидуально без отношения к другим пакетам, несмотря на то что они могут являться частью одного трафика.

Достоинства пакетных фильтров:

– дешевле, чем другие методы проверки пакета;

– являются независимыми от приложения, так как их решения основаны на информации, содержащейся в заголовке пакета, а не на информации, которая имеет отношение к определенному приложению.

Недостатки пакетных фильтров:

– если порт был открыт МСЭ, то он открыт для всех проходящих трафиков через этот порт;

– проверка точности выполнения правил на пакетном фильтре является очень трудной задачей. Даже если правила кажутся простыми и явными, проверка их правильности путѐм тестирования отнимает много времени и не всегда дает правильный результат.

МСЭ с контролем состояния исследует информацию заголовков пакетов от сетевого уровня до прикладного уровня модели OSI и проверяет, что данный пакет является частью законного потока и используются допустимые протоколы.

Достоинства МСЭ с контролем состояния:

– оказывают очень небольшое влияние на работу сети, они реализуются прозрачно и являются независимыми от приложений;

– более безопасны, чем пакетные фильтры;

– анализируя информацию заголовка пакета, может проверить, что протоколы прикладного уровня работают правильно.

Недостатки МСЭ с контролем состояния:

– не нарушает модель «клиент-сервер» и разрешает прямое соединение между двумя конечными точками;

– правила и фильтры этого метода могут быть достаточно сложными и трудными для восприятия.

Прокси-серверы обычно реализуются на безопасной системе хоста, формируемой с двумя интерфейсами сети. Прокси-серверы являются посредниками между этими двумя конечными точками. Этот метод проверки пакета нарушает модель «клиент-сервер» и осуществляет вместо этой модели две связи: первая связь от источника к прокси-серверу и вторая от прокси-сервера к назначению. Каждая конечная точка может общаться с другими точками, только проходя прокси-сервер.

Достоинства прокси-серверов:

– не позволяют прямую связь между конечными точками;

– не реализуют прямой маршрут между сетями;

– позволяют администраторам сети иметь больше контроля над трафиком, проходящим через межсетевой экран;

– есть лучшие способности фильтрования.

Недостатки прокси-серверов:

– весь исходящий и входящий трафик проверяется на прикладном уровне, поэтому они медленнее, чем другие типы МСЭ;

– каждый протокол требует привязки к прокси-серверу. Если такой привязки не существует, то соответствующий протокол не может проходить через МСЭ.

МСЭ представляет собой эффективное средство, реализующее контроль за информацией, поступающей в локальную сеть и (или) выходящей из нее, посредством анализа по совокупности критериев и правил принятия решения о ее распространении в локальной сети.

Библиографический список

1. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – Москва, 1997.

Образец цитирования:

Власова, В. А. Проект модуля межсетевого экрана в составе устройства – маршрутизатора сетевых пакетов / В. А. Власова, В. Б. Варламов // Инжиниринг и технологии. – 2019. – Vol. 4(1). – С. 1–2. – DOI 10.21685/2587-7704-2019-4-1-3.