МЕТОДИКА РАЗВЕРТЫВАНИЯ И КОНФИГУРИРОВАНИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сакович Д. А.

Бобов М. Н. – д-р. техн. наук, профессор

Межсетевой экран представляет собой специальное решение для обеспечения безопасности сети. Его функция заключается в постоянном мониторинге входящего и исходящего трафика и его фильтрации на основании установленных правил. Благодаря этому обеспечивается создание защитной стены между внутренней и внешней сетью.

При выборе межсетевого экрана для развертывания необходимо учесть следующие моменты:

- Необходимая категория межсетевых экранов – оборудование, программное обеспечение, программно-аппаратных комплекс.
- Особенности конфигурации сети, которые могут повлиять на выбор межсетевого экрана, например, необходимость поддержки заданного количества пользовательских сессий без ущерба производительности, возможность организации подсетей и другие.
- Используемые механизмы сетевой безопасности - возможности межсетевого экрана и способность решать конкретные задачи.
- Пропускная способность и ее параметры при разных режимах работы.
- Количество портов LAN, WAN, DMZ.
- Особенности конструктивного исполнения (для оборудования).
- Затраты на покупку, эксплуатацию, обслуживание.

Различают следующие типы межсетевых экранов[1][2]:

- Управляемые коммутаторы.
- Пакетные фильтры.
- Шлюзы сеансового уровня.
- Посредники прикладного уровня.
- Инспекторы состояния.
- Управляемые коммутаторы

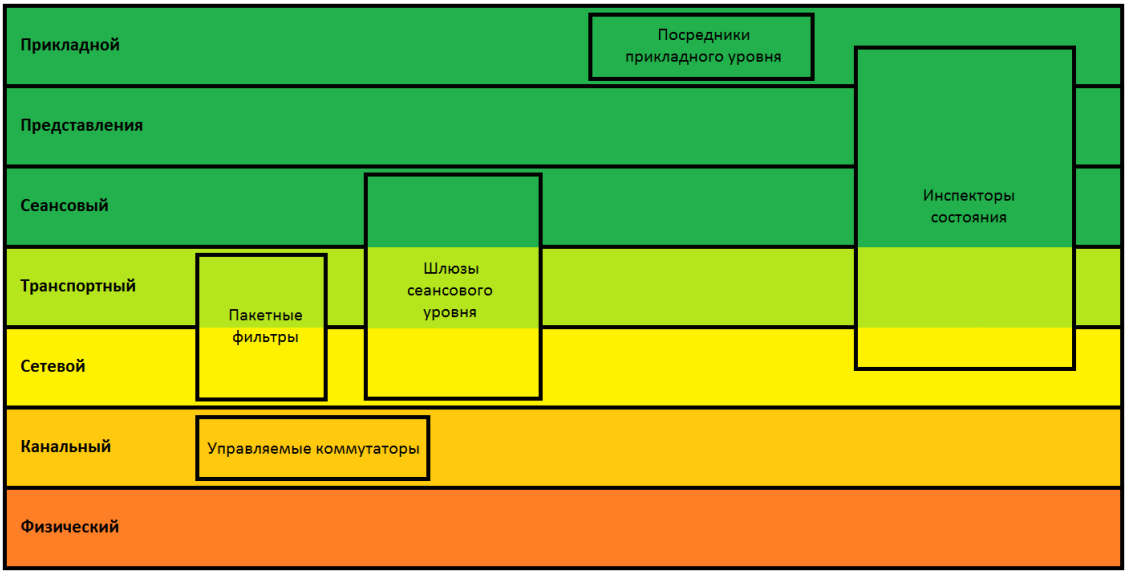

Рисунок 1 – Схематическое изображение классификации межсетевых экранов на основе сетевой модели OSI

При реализации политики безопасности в рамках корпоративной сети, основу которых составляют управляемые коммутаторы, они могут быть мощным и достаточно дешёвым решением. Взаимодействуя только с протоколами канального уровня, такие межсетевые экраны фильтруют трафик с очень высокой скоростью. Основным недостатком такого решения является невозможность анализа протоколов более высоких уровней[2].

Пакетные фильтры функционируют на сетевом уровне и контролируют прохождение трафика на основе информации, содержащейся в заголовке пакетов. Многие межсетевые экраны данного типа могут оперировать заголовками протоколов и более высокого, транспортного, уровня (например, TCP или UDP). Пакетные фильтры одними из первых появились на рынке межсетевых экранов и по сей день остаются самым распространённым их типом. Данная технология реализована в подавляющем большинстве маршрутизаторов и даже в некоторых коммутаторах[3].

Межсетевой экран сеансового уровня исключает прямое взаимодействие внешних хостов с узлом, расположенным в локальной сети, выступая в качестве посредника (англ. proxy), который реагирует на все входящие пакеты и проверяет их допустимость на основании текущей фазы соединения. Шлюз сеансового уровня гарантирует, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению [1].

Так как межсетевой экран данного типа исключает прямое взаимодействие между двумя узлами, шлюз сеансового уровня является единственным связующим элементом между внешней сетью и внутренними ресурсами. Это создаёт видимость того, что на все запросы из внешней сети отвечает шлюз, и делает практически невозможным определение топологии защищаемой сети. Кроме того, так как контакт между узлами устанавливается только при условии его допустимости, шлюз сеансового уровня предотвращает возможность реализации DoS-атаки, присущей пакетным фильтрам.

Посредники прикладного уровня

Межсетевые экраны прикладного уровня, к которым, в частности, относится файрвол веб-приложений, как и шлюзы сеансового уровня, исключают прямое взаимодействие двух узлов. Однако, функционируя на прикладном уровне, они способны «понимать» контекст передаваемого трафика. Межсетевые экраны, реализующие эту технологию, содержат несколько приложений-посредников, каждое из которых обслуживает свой прикладной протокол. Такой межсетевой экран способен выявлять в передаваемых сообщениях и блокировать несуществующие или нежелательные последовательности команд, что зачастую означает DoS-атаку, либо запрещать использование некоторых команд (например, FTP PUT, которая даёт возможность пользователю записывать информацию на FTP сервер).

Посредники прикладного уровня способны выполнять аутентификацию пользователя, а также проверять, что SSL-сертификаты подписаны конкретным центром. Межсетевые экраны прикладного уровня доступны для многих протоколов, включая HTTP, FTP, почтовые (SMTP, POP, IMAP), Telnet и другие[2].

Инспекторы состояния

Каждый из вышеперечисленных типов межсетевых экранов используется для защиты корпоративных сетей и обладает рядом преимуществ. Однако, куда эффективней было бы собрать все эти преимущества в одном устройстве и получить межсетевой экран, осуществляющий фильтрацию трафика с сетевого по прикладной уровень. Данная идея была реализована в инспекторах состояний, совмещающих в себе высокую производительность и защищённость.

Осуществляя фильтрацию трафика по принципу шлюза сеансового уровня, данный класс межсетевых экранов не вмешивается в процесс установления соединения между узлами. Поэтому производительность инспектора состояний заметно выше, чем у посредника прикладного уровня и шлюза сеансового уровня, и сравнима с производительностью пакетных фильтров [1].

Межсетевые экраны не являются панацеей при борьбе с атаками злоумышленников. Они не могут предотвратить атаки внутри локальной сети, но вместе с другими средствами защиты играют исключительно важную роль для защиты сетей от вторжения извне. Понимание технологии работы межсетевых экранов позволяет не только сделать правильный выбор при покупке системы защиты, но и корректно настроить межсетевой экран.

Список использованных источников:

1. Лебедь С. В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. — МГТУ им. Н. Э. Баумана, 2002. — 306 с.

2. Чепмен-мл. Д. В., Фокс Э. Брандмауэры Cisco Secure PIX = Cisco® Secure PIX® Firewalls. — Вильямс, 2003

3. Фаронов А. Е. Основы информационной безопасности при работе на компьютере. — ИНТУИТ, 2016. — 155 с.