УДК 621.391

МЕЖСЕТЕВЫЕ ЭКРАНЫ

Ф.О. МОХАММЕД

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6 Минск 220013, Беларусь

Поступила в редакцию 26 октября 2009

Используемые межсетевым экраном механизмы служат для предотвращения или блокирования нежелательного трафика. Такими механизмами, могут быть: простой пакетный фильтр, который принимает решения в зависимости от содержания заголовка пакета; или анализатор состояния который проверяет, что данный пакет является частью законного потока; или более сложный механизм такой как прокси-сервер который устанавливается между клиентом и внешней сетью.

Ключевые слова: межсетевой экран (МСЭ), пакетный фильтр, контроль состояния, прокси-сервер.

Введение

Межсетевые экраны обеспечивают барьер между сетями и предотвращают или блокируют нежелательный или несанкционированный трафик. Единственного определения для межсетевого экрана не существует. В данной работе будем использовать следующее определение межсетевого экрана. Межсетевой экран – система или группа систем, используемая для управления доступом между доверенными и не доверенными сетями на основе предварительно сконфигурированных правил [1].

Межсетевые экраны могут управлять доступом к сети и от нее. Они могут настраиваться для предотвращения получения доступа к внутренним сетям и услугам несанкционированных пользователей. Они могут также конфигурироваться для предотвращения нежелательного доступа к внешним или несанкционированным сетям и услугам внутренних пользователей. МСЭ обеспечивает также выполнение следующих функций:

Установление подлинности пользователя: межсетевые экраны могут настраиваться для обеспечения установления подлинности пользователя. Это позволяет администраторам сетей управлять доступом определенных пользователей к определенным услугам и ресурсам. Установление подлинности также позволяет администраторам сетей отслеживать определенную деятельность пользователя и попытки получить несанкционированный доступ к защищенным сетям или услугам.

Аудит и регистрация: межсетевые экраны могут обеспечить аудит и регистрацию действий, сохранить и проанализировать эту информацию позднее. Межсетевые экраны тоже могут произвести статистику, основанную на информации, которую они собирают. Эти статистические данные очень полезны администраторами безопасности при принятии решений.

Безопасность: некоторые функции межсетевых экранов позволяют скрыть внутренние или доверенные сети, от внешних или не доверенных сетей. Это помогает в ограждении услуг от нежелательных просмотров. Когда людские и финансовые ресурсы ограничены, межсетевые экраны могут являться центральной точкой управления безопасности.

Наряду с достоинствами межсетевые экраны обладают рядом недостатков:

Транспортные узкие места: в некоторых сетях межсетевые экраны создают транспортное узкое место. Они вынуждают все межсетевые трафики проходить через межсетевой экран, поэтому есть большая вероятность, что сеть станет переполненной.

Единственный пункт отказа: межсетевые экраны могут создать единственный пункт отказа. В большинстве конфигураций, где межсетевые экраны являются единственной связью между сетями, если они недоступны или конфигурируются не правильно, то никакой трафик через них не пройдет.

Повешенная ответственность администратора: межсетевой экран часто добавляет ответственность в управление сетью и делает обслуживание сети более сложным, потому что все межсетевые экраны требуют длительной административной поддержки в виде обновлений программного обеспечения и перенастройки политик безопасности.

Для управления доступом к сети, межсетевые экраны используют один из двух принципов защиты:

1. Все неопределенно разрешенное, запрещено.
2. Все неопределенно запрещённое, разрешено.

У каждого принципа есть сторонники, но первый принцип чаще всего рекомендуемый. Он базируется на предпосылке, что если определенные правила разрешения отсутствуют, то доступ запрещен.

Второй принцип имеет противоположную логику. Доступ запрещается, если для этого сформированы определенные правила. Если правил нет, то доступ полностью открыт.

Типы межсетевых экранов

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:

1. Пакетные фильтры (Packet filtering),
2. МСЭ с контролем состояния (Stateful packet inspection),
3. Прикладной шлюз/прокси (Application gateways/proxies).

Гибридные методы проверки пакетов комбинируют два или более из них для обеспечения повышенных возможностей и безопасности.

Пакетные фильтры

Пакетные фильтры (рис. 1) – 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 [2].

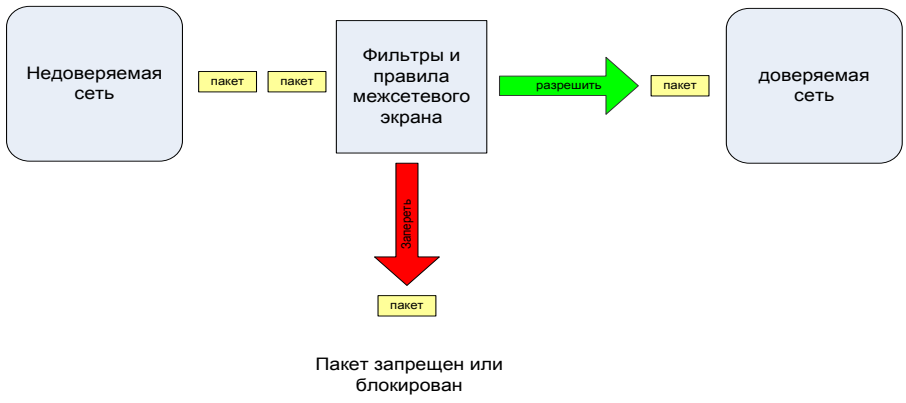

Рис. 1. Межсетевой экран – пакетный фильтр

Пакетные фильтры часто называют межсетевыми экранами уровня сети, потому что процесс фильтрования происходит на сетевом уровне (третий уровень) или транспортным уровне (четвертый уровень) модели OSI. Рис. 2 показывает отношение между пакетным фильтром и моделью OSI [3, 4].

Рис. 2. Пакетный фильтр и уровни OSI

Правила пакетной фильтрации или фильтры могут быть сконфигурированы на основе разрешения или запрета. Конфигурация правил фильтрования пакета основывается на одном или более следующих параметров:

- IP адрес источника,
- IP адрес назначения,
- Тип протокола,
- Порт источника,
- Порт назначения.

Достоинства

Пакетные фильтры функционируют быстрее, чем другие типы МСЭ, так как фильтруют пакеты на более низких уровнях модели OSI. Если они настроены правильно, то пакетные фильтры оказывают очень малое влияние на работу сети.

Пакетные фильтры могут быть установлены прозрачным образом. Они не требуют никакой дополнительной конфигурации для клиентов.

Пакетные фильтры межсетевых экранов дешевле, чем другие методы проверки пакета.

Пакетные фильтры 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

Если порт был открыт МСЭ, то он открыт для всех проходящих трафиков через этот порт.

Определение правил и фильтров в этом методе является сложной задачей. У администратора сети должно быть хорошее понимание услуг и протоколов для выполнения требования безопасности.

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

МСЭ с контролем состояния

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. рис. 3 показывает отношению между МСЭ с контролем состояния и моделью OSI.

Рис. 3. МСЭ с контролем состояния и уровни OSI

МСЭ с контролем состояния работает следующим образом (рис. 4). Заголовки TCP пакета проверяются для определения, является ли пакет частью уже существующего и действующего потока передаваемых данных. Межсетевой экран имеет активную таблицу всех текущих сеансов и сравнивает входящие пакеты с её данными в процессе контроля доступа. Если в таблице отсутствует соответствующий вход соединения, МСЭ проверяет пакет с использованием установленного набора правил, аналогичного фильтру пакетов. Если проверка по правилам фильтрации прошла успешно и передача пакета разрешается, МСЭ создает или обновляет свою таблицу соединений. Внесенный вход соединения будет использоваться для проверки последующих пакетов вместо правил фильтрации. В качестве параметров проверки состояния используются:

- IP адрес источника,
- IP адрес назначения,
- Тип Протокола,
- Порт источника,
- Порт назначения,
- Состояние связи.

Состояние связи определяется из информации собранной на основе анализа предыдущих пакетов. Это - существенный фактор в принятии решения при новых попытках открыть соединение. МСЭ с контролем состояния сравнивает пакеты с правилами или фильтрами и затем по динамической таблице состояния, проверяет, что все пакеты - часть действительной и установленной связи.

Этот метод защищает сети от атаки лучше, чем методы экранирования пакетов, потому что он имеет возможность анализа состояния связи.

Достоинства

МСЭ с контролем состояния, как и пакетные фильтры, оказывают очень небольшое влияние на работу сети, они реализуется прозрачно, и являются независимыми от приложений.

МСЭ с контролем состояния более безопасны, чем пакетные фильтры. Так как производят более глубокий анализ заголовка пакета для определения состояния связи между конечными точками.

Анализируя информацию заголовка пакета, МСЭ с контролем состояния может проверить, что протоколы прикладного уровня работают правильно.

У МСЭ с контролем состояния обычно есть некоторые возможности по регистрации. Регистрация может помочь идентифицировать и отследить различные типы трафиков, проходящие через межсетевой экран.

Недостатки

Как и пакетные фильтры, МСЭ с контролем состояния не нарушает модель клиент/сервер и разрешает прямое соединение между этими двумя конечными точками.

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

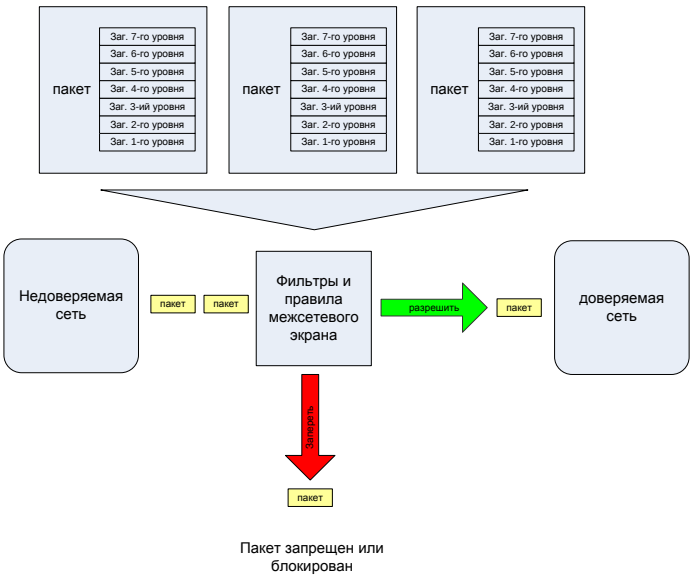

Рис. 4. МСЭ с контролем состояния

Прокси-серверы

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.

Этот тип межсетевого экрана работает на прикладном уровне модели OSI. Для соединения конечных точек источников с точками назначений, прокси-сервер должен быть реализован в каждом протоколе прикладного уровня. Рис. 5 показывает отношения между прокси-серверами и моделью OSI.

Прикладной	Прокси-серверы
Представит.	
Сеансовый	
Транспортный	
Сетевой	
Канальный	
Физический	

Рис. 5. Прокси-серверы и уровни OSI

Прокси-сервер работает следующим образом (рис. 6). Когда клиент делает запрос из недоверяемой сети, связь устанавливается с прокси-сервером. Прокси-сервер определяет, действителен ли запрос (сравнивая его с правилами или фильтрами) и затем посылает новый запрос от себя к назначению. При использовании этого метода прямая связь от доверяемой сети до недоверяемой сети, никогда не осуществляется, и запрос представляется пришедшим от прокси-сервера.

Ответ отсылается назад к прокси-серверу и затем пересылается клиенту. Нарушая модель клиент-сервер, этот тип межсетевого экрана может эффективно скрыть доверяемую сеть от недоверяемой сети.

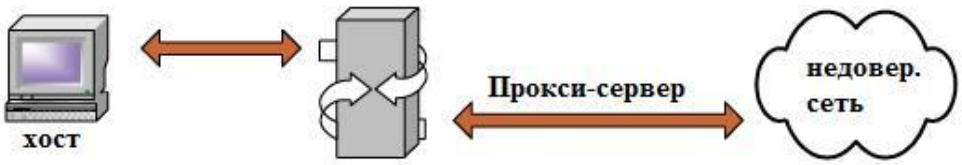

Рис. 6. Прокси-сервер межсетевой экран

В отличие от пакетного фильтра и МСЭ с контролем состояния, прокси-сервер может видеть все аспекты прикладного уровня, и таким образом может исследовать более определенную информацию. Например, он может найти различие между частью электронной почты содержащей текст и содержащей графическое изображение, или различие между веб-страницами (web page) с использованием языка Java и веб-страницами без Явы. С точки зрения безопасности прокси-серверы выше других типов экранирования пакета, Но этот метод не всегда является самым практичным для использования.

Достоинства

Прокси-сервер не позволяет прямую связь между конечными точками. Он нарушает модель клиент-сервер. В этом отношении, этот метод действительно разделяет внутренние и внешние сети.

Прокси-сервер не реализует прямой маршрут между сетями. Так как никакая маршрутизация не делается, этот метод обеспечивает трансляцию сетевых адресов (Network Address Translation (NAT)).

Прокси-серверы позволяют администратору сети иметь больше контроля над трафиком, проходящим через межсетевой экран. Они могут разрешить или запретить определенные приложения или определенные особенности приложений.

У прокси-серверов есть лучшие способности фильтрования. Так как у них есть способность исследовать информационную часть пакета, они способны к принятию решений, основанному на содержании.

Недостатки

На прокси-серверах весь исходящий и входящий трафик проверяется на прикладном уровне, поэтому они медленнее, чем пакетные фильтры и МСЭ с контролем состояния, которые проверяют трафик на сетевом уровне. В этом методе все трафики должны пройти через все уровни модели OSI, в результате инспекционный процесс требует много времени обработки. Это может привести и тому, что МСЭ может стать узким местом в сети.

Другой недостаток прокси-сервера состоит в том, что каждый протокол требует своей собственной привязки к прокси-серверу. Если такой привязки не существует, то соответствующий протокол не может проходить через межсетевой экран. Кроме того, так как для каждого протокола требуется свой собственный прокси-сервер, поддержка новых протоколов может стать трудным делом.

Прокси-серверы требуют дополнительных конфигураций клиента. Клиентам на сети может потребоваться специализированное программное обеспечение, чтобы быть в состоянии соединиться с прокси-сервером. Это может оказать сильное влияние на большие сети с многочисленными клиентами.

Масштабируемость может быть проблемой с прокси-серверами, когда они установлены в больших сетях. Потому что, если число клиентов или число прокси-серверов расположенных на одном хосте увеличивается, то работа ухудшается.

Прокси-серверы, установленные на операционных системах общего назначения, уязвимы для лазеек безопасности основной системы. Если основная система не безопасна, то межсетевой экран не безопасен.

Заключение

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.

FIREWALLS

F. O. MOHAMMED

Abstract

The mechanisms that used by the firewall to allow or block traffic can be simple packet filters, which make decisions based on the contents of the packet header, or stateful packet inspection which checks the state of all current connections, or more complex application proxies, which stand between the client and the outside world, acting as a middleman for some network services.

Литература

1. *David Hucaby*. Cisco ASA, PIX, and FWSM Firewall Handbook // Cisco press, Second Edition. 2008.
2. *Vitaly Osipov, Mike Sweenety,Woody Weaver, Charles E. Riley, Umer Khan*. // Cisco Security Specialist's guide to PIX Firewall. 2002.
3. *Terry Ogletree*. // Practical Firewalls. 2000.
4. *Wes Noonan, Ido Dubrawsky*. // Firewall Fundamentals. 2006.