10. Лекция: Межсетевые экраны

В лекции рассмотрены различные типы межсетевых экранов и их различные архитектуры.

Межсетевой экран (firewall) - это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных. Этим оно отличается от маршрутизатора, функцией которого является доставка трафика в пункт назначения в максимально короткие сроки.

Существует мнение, что маршрутизатор также может играть роль межсетевого экрана. Однако между этими устройствами существует одно принципиальное различие: маршрутизатор предназначен для быстрой маршрутизации трафика, а не для его блокировки. Межсетевой экран представляет собой средство защиты, которое пропускает определенный трафик из потока данных, а маршрутизатор является сетевым устройством, которое можно настроить на блокировку определенного трафика.

Кроме того, межсетевые экраны, как правило, обладают большим набором настроек. Прохождение трафика на межсетевом экране можно настраивать по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих службу. Межсетевые экраны позволяют осуществлять централизованное управление безопасностью. В одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Это не устраняет потребность в обновлении и настройке систем, но позволяет снизить вероятность неправильного конфигурирования одной или нескольких систем, в результате которого эти системы могут подвергнуться атакам на некорректно настроенную службу.

Определение типов межсетевых экранов

Существуют два основных типа межсетевых экранов: межсетевые экраны прикладного уровня и межсетевые экраны с пакетной фильтрацией. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика. Из материала следующих разделов вы увидите, что степень обеспечиваемой этими устройствами защиты зависит от того, каким образом они применены и настроены.

Межсетевые экраны прикладного уровня

Межсетевые экраны прикладного уровня, или прокси-экраны, представляют собой программные пакеты, базирующиеся на операционных системах общего назначения (таких как Windows NT и Unix) или на аппаратной платформе межсетевых экранов. Межсетевой экран обладает несколькими интерфейсами, по одному на каждую из сетей, к которым он подключен. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствует явное разрешение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты.

Правила политики безопасности усиливаются посредством использования модулей доступа. В межсетевом экране прикладного уровня каждому разрешаемому протоколу должен соответствовать свой собственный модуль доступа. Лучшими модулями доступа считаются те, которые построены специально для разрешаемого протокола. Например, модуль доступа FTP предназначен для протокола FTP и может определять, соответствует ли проходящий трафик этому протоколу и разрешен ли этот трафик правилами политики безопасности.

При использовании межсетевого экрана прикладного уровня все соединения проходят через него (см. рис. 10.1). Как показано на рисунке, соединение начинается на системе-клиенте и поступает на внутренний интерфейс межсетевого экрана. Межсетевой экран принимает соединение, анализирует содержимое пакета и используемый протокол и определяет, соответствует ли данный трафик правилам политики безопасности. Если это так, то межсетевой экран инициирует новое соединение между своим внешним интерфейсом и системой-сервером.

Межсетевые экраны прикладного уровня используют модули доступа для входящих подключений. Модуль доступа в межсетевом экране принимает входящее подключение и обрабатывает команды перед отправкой трафика получателю. Таким образом, межсетевой экран защищает системы от атак, выполняемых посредством приложений.

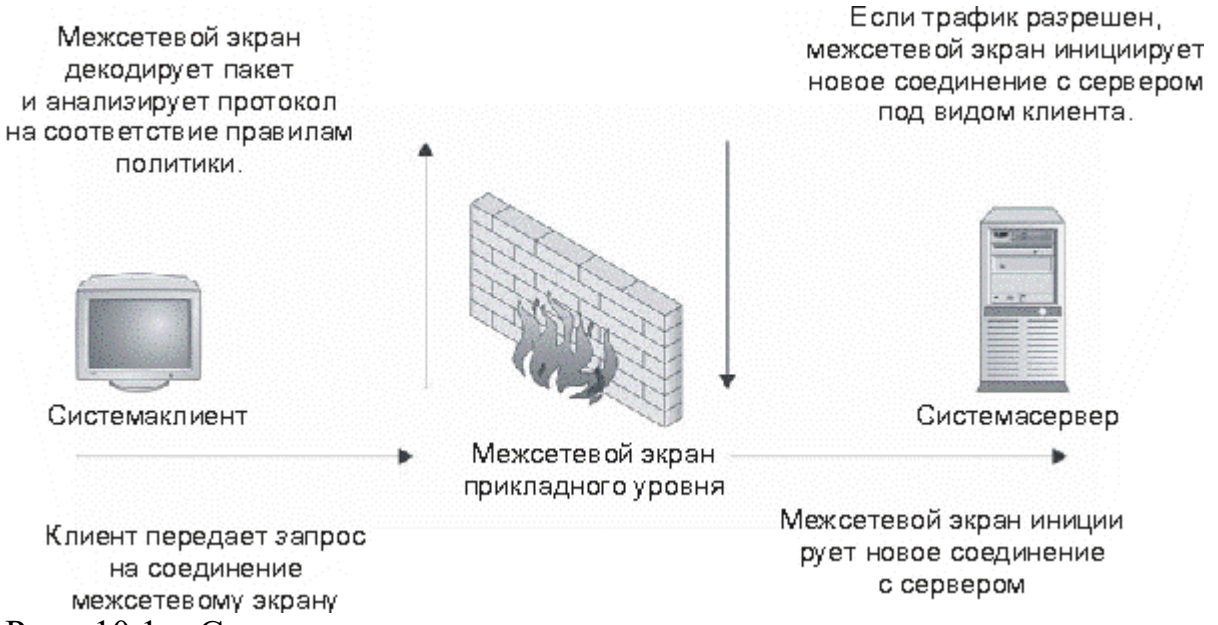

Рис. 10.1. Соединения модуля доступа межсетевого экрана прикладного уровня

Примечание

Здесь подразумевается, что модуль доступа на межсетевом экране сам по себе неуязвим для атаки. Если же программное обеспечение разработано недостаточно тщательно, это может быть и ложным утверждением.

Дополнительным преимуществом архитектуры данного типа является то, что при ее использовании очень сложно, если не невозможно, "скрыть" трафик внутри других служб. Например, некоторые программы контроля над системой, такие как NetBus и Back Orifice, могут быть настроены на использование любого предпочитаемого пользователем порта. Следовательно, их можно настроить на использование порта 80 (HTTP). При использовании правильно настроенного межсетевого экрана прикладного уровня модуль доступа не сможет распознавать команды, поступающие через соединение, и соединение, скорее всего, не будет установлено.

Межсетевые экраны прикладного уровня содержат модули доступа для наиболее часто используемых протоколов, таких как HTTP, SMTP, FTP и telnet. Некоторые модули доступа могут отсутствовать. Если модуль доступа отсутствует, то конкретный протокол не может использоваться для соединения через межсетевой экран.

Межсетевой экран также скрывает адреса систем, расположенных по другую сторону от него. Так как все соединения инициируются и завершаются на интерфейсах межсетевого экрана, внутренние системы сети не видны напрямую извне, что позволяет скрыть схему внутренней адресации сети.

Примечание

Большая часть протоколов прикладного уровня обеспечивает механизмы маршрутизации к конкретным системам для трафика, направленного через определенные порты. Например, если весь трафик, поступающий через порт 80, должен направляться на веб-сервер, это достигается соответствующей настройкой межсетевого экрана.

Межсетевые экраны с пакетной фильтрацией

Межсетевые экраны с пакетной фильтрацией могут также быть программными пакетами, базирующимися на операционных системах общего назначения (таких как Windows NT и Unix) либо на аппаратных платформах межсетевых экранов. Межсетевой экран имеет несколько интерфейсов, по одному на каждую из сетей, к которым подключен экран. Аналогично межсетевым экранам прикладного уровня, доставка трафика из одной сети в другую определяется набором правил политики. Если правило не разрешает явным образом определенный трафик, то соответствующие пакеты будут отклонены или аннулированы межсетевым экраном.

Правила политики усиливаются посредством использования фильтров пакетов. Фильтры изучают пакеты и определяют, является ли трафик разрешенным, согласно правилам политики и состоянию протокола (проверка с учетом состояния). Если протокол приложения функционирует через TCP, определить состояние относительно просто, так как TCP сам по себе поддерживает состояния. Это означает, что когда протокол находится в определенном состоянии, разрешена передача только определенных пакетов. Рассмотрим в качестве примера последовательность установки соединения. Первый ожидаемый пакет - пакет SYN. Межсетевой экран обнаруживает этот пакет и переводит соединение в состояние SYN. В данном состоянии ожидается один из двух пакетов - либо SYN ACK (опознавание пакета и разрешение соединения) или пакет RST (сброс соединения по причине отказа в соединении получателем). Если в данном соединении появятся другие пакеты, межсетевой экран аннулирует или отклонит их, так как они не подходят для данного состояния соединения, даже если соединение разрешено набором правил.

Если протоколом соединения является UDP, межсетевой экран с пакетной фильтрацией не может использовать присущее протоколу состояние, вместо чего отслеживает состояние трафика UDP. Как правило, межсетевой экран принимает внешний пакет UDP и ожидает входящий пакет от получателя, соответствующий исходному пакету по адресу и порту, в течение определенного времени. Если пакет принимается в течение этого отрезка времени, его передача разрешается. В противном случае межсетевой экран определяет, что трафик UDP не является ответом на запрос, и аннулирует его.

При использовании межсетевого экрана с пакетной фильтрацией соединения не прерываются на межсетевом экране (см. рис. 10.2), а направляются непосредственно к конечной системе. При поступлении пакетов межсетевой экран выясняет, разрешен ли данный пакет и состояние соединения правилами политики. Если это так, пакет передается по своему маршруту. В противном случае пакет отклоняется или аннулируется.

Рис. 10.2. Передача трафика через межсетевой экран с фильтрацией пакетов

Межсетевые экраны с фильтрацией пакетов не используют модули доступа для каждого протокола и поэтому могут использоваться с любым протоколом, работающим через IP. Некоторые протоколы требуют распознавания межсетевым экраном выполняемых ими действий. Например, FTP будет использовать одно соединение для начального входа и команд, а другое - для передачи файлов. Соединения, используемые для передачи файлов, устанавливаются как часть соединения FTP, и поэтому межсетевой экран должен уметь считывать трафик и определять порты, которые будут использоваться новым соединением. Если межсетевой экран не поддерживает эту функцию, передача файлов невозможна.

Как правило, межсетевые экраны с фильтрацией пакетов имеют возможность поддержки большего объема трафика, т. к. в них отсутствует нагрузка, создаваемая дополнительными процедурами настройки и вычисления, имеющими место в программных модулях доступа.

Примечание

Последний абзац начинается с фразы "как правило". Различные производители межсетевых экранов сопоставляют их производительность различными способами. Исторически сложилось так, что межсетевые экраны с пакетной фильтрацией имеют возможность обработки большего объема

трафика, нежели межсетевые экраны прикладного уровня, на платформе одного и того же типа. Это сравнение показывает различные результаты в зависимости от типа трафика и числа соединений, имеющих место в процессе тестирования.

Межсетевые экраны, работающие только посредством фильтрации пакетов, не используют модули доступа, и поэтому трафик передается от клиента непосредственно на сервер. Если сервер будет атакован через открытую службу, разрешенную правилами политики межсетевого экрана, межсетевой экран никак не отреагирует на атаку. Межсетевые экраны с пакетной фильтрацией также позволяют видеть извне внутреннюю структуру адресации. Внутренние адреса скрывать не требуется, так как соединения не прерываются на межсетевом экране.

Гибридные межсетевые экраны

Как и многие другие устройства, межсетевые экраны изменяются и совершенствуются с течением времени, т. е. эволюционируют. Производители межсетевых экранов прикладного уровня в определенный момент пришли к выводу, что необходимо разработать метод поддержки протоколов, для которых не существует определенных модулей доступа. Вследствие этого увидела свет технология модуля доступа Generic Services Proxy (GSP). GSP разработана для поддержки модулями доступа прикладного уровня других протоколов, необходимых системе безопасности и при работе сетевых администраторов. В действительности GSP обеспечивает работу межсетевых экранов прикладного уровня в качестве экранов с пакетной фильтрацией.

Производители межсетевых экранов с пакетной фильтрацией также добавили некоторые модули доступа в свои продукты для обеспечения более высокого уровня безопасности некоторых широко распространенных протоколов. На сегодняшний день многие межсетевые экраны с пакетной фильтрацией поставляются с модулем доступа SMTP.

В то время как базовая функциональность межсетевых экранов обоих типов осталась прежней, (что является причиной большинства "слабых мест" этих устройств), сегодня на рынке присутствуют гибридные межсетевые экраны. Практически невозможно найти межсетевой экран, функционирование которого построено исключительно на прикладном уровне или фильтрации пакетов. Это обстоятельство отнюдь не является недостатком, так как оно позволяет администраторам, отвечающим за безопасность, настраивать устройство для работы в конкретных условиях.

Вопросы для самопроверки

1. Межсетевой экран, использующий модули доступа для контроля за соединениями, называется _____.
2. Что проверяет межсетевой экран с фильтрацией пакетов, помимо набора правил, для принятия решения о блокировке или передаче пакета?

Разработка конфигурации межсетевого экрана

Теперь давайте рассмотрим некоторые стандартные сетевые архитектуры и выясним, каким образом следует настраивать сетевой экран в той или иной конкретной ситуации. В этом упражнении подразумевается, что в организации присутствуют указанные ниже системы, и что эти системы принимают входящие соединения из интернета:

- веб-сервер, работающий только через порт 80;
- почтовый сервер, работающий только через порт 25. Он принимает всю входящую и отправляет всю исходящую почту. Внутренний почтовый сервер периодически связывается с данной системой для получения входящей почты и отправки исходящих сообщений.

Существует внутренняя система DNS, которая запрашивает системы интернета для преобразования имен в адреса, однако в организации отсутствует своя собственная главная внешняя DNS.

Интернет-политика организации позволяет внутренним пользователям использовать следующие службы:

- HTTP;
- HTTPS;
- FTP;
- Telnet;
- SSH.

На базе этой политики можно построить правила политики для различных архитектур.

Архитектура 1: системы за пределами межсетевого экрана, доступные из интернета

На рис. 10.3 показано размещение доступных из интернета систем между сетевым экраном и внешним маршрутизатором. В таблице 10.1 приведены правила межсетевого экрана.

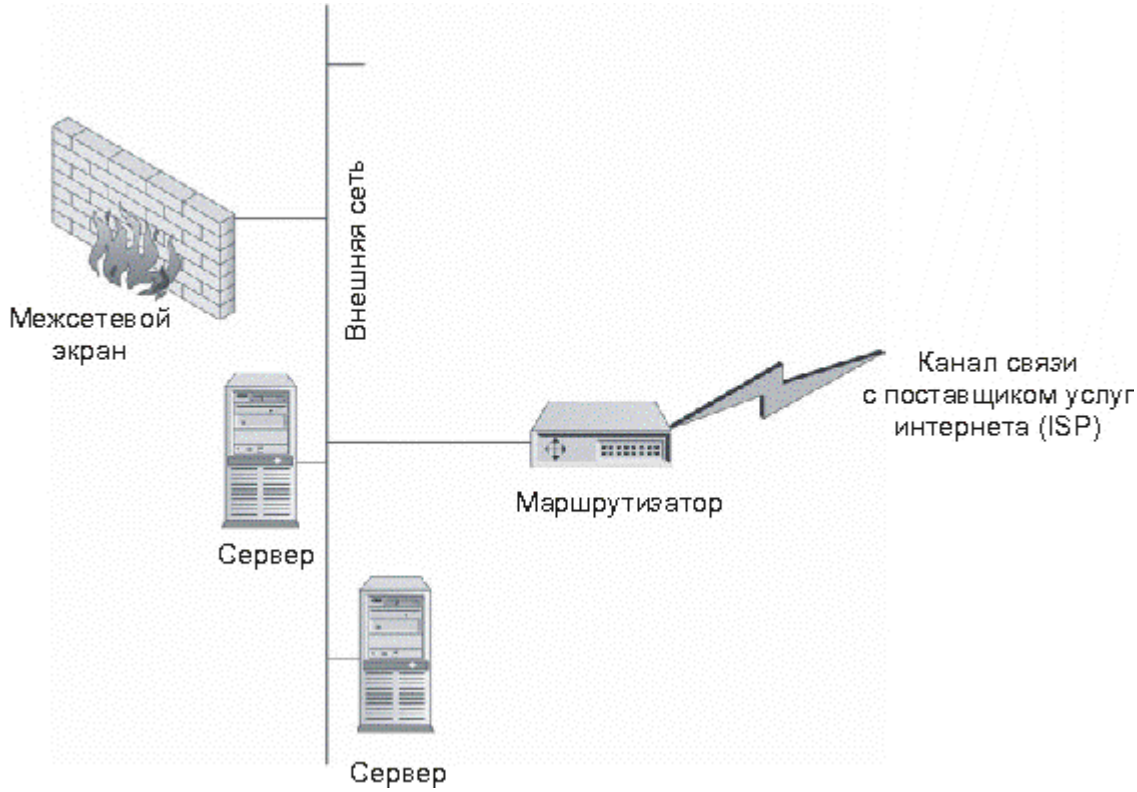

Рис. 10.3. Системы за пределами межсетевого экрана, доступные из интернета

На маршрутизаторе может быть установлена фильтрация, позволяющая только внешним данным HTTP поступать на веб-сервер и передавать на почтовый сервер только поступающие извне данные SMTP. Как видно из приведенных правил, независимо от того, какой тип межсетевого экрана используется, веб-сервер и почтовый сервер не защищены межсетевым экраном. В данном случае межсетевой экран лишь защищает внутреннюю сеть организации.

Таблица 10.1. Правила межсетевого экрана для расположенных за пределами межсетевого экрана систем, доступных из интернета

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Внутренний почтовый сервер	Почтовый сервер	SMTP	Принятие
2	Внутренняя сеть	Почтовый сервер	Любой HTTP, HTTPS, FTP, telnet, SSH	Принятие
3	Внутренняя DNS	Любой	DNS	Принятие
4	Любой	Любой	Любая	Сброс

Архитектура 2: один межсетевой экран

Вторая стандартная архитектура показана на рис. 10.4. В данной архитектуре используется один межсетевой экран для защиты как внутренней сети, так и

любых других систем, доступных из интернета. Эти системы располагаются в отдельной сети. В таблице 10.2 приведены правила межсетевого экрана.

Рис. 10.4. Один межсетевой экран

Таблица 10.2. Правила межсетевого экрана для архитектуры с одним межсетевым экраном

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Любой	Веб-сервер	HTTP	Принятие
2	Любой	Почтовый сервер	SMTP	Принятие
3	Почтовый сервер	Любой	SMTP	Принятие
4	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, telnet, SSH	Принятие
5	Внутренняя DNS	Любой	DNS	Принятие
6	Любой	Любой	Любая	Сброс

Как видно из таблицы 10.2, правила практически аналогичны правилам архитектуры 1. Межсетевой экран дополняет правила, которые использовались в маршрутизаторе в предыдущей архитектуре. Также мы видим, что не существует явного правила, позволяющего внутреннему почтовому серверу подключаться к почтовому серверу в отдельной сети. Причиной этому является правило 2, позволяющее любой системе (внутренней или внешней) подключаться к упомянутой системе.

Архитектура 3: двойные межсетевые экраны

Третья архитектура, о которой пойдет речь, использует двойные межсетевые экраны (см. рис. 10.5). Доступные из интернета системы располагаются между межсетевыми экранами, а внутренняя сеть расположена за вторым межсетевым экраном. В таблице 10.3 приведены правила для межсетевого экрана 1.

Вопрос к эксперту

Вопрос. Используются ли межсетевые экраны только на соединениях с интернетом?

Ответ. Не следует ограничивать область действия межсетевых экранов одними лишь интернет-соединениями. Межсетевой экран представляет собой устройство, которое может использоваться в любой ситуации, требующей контроля доступа. В частности, данные устройства можно использовать во внутренних сетях, которые необходимо защищать от других внутренних систем. Секретные внутренние сети могут содержать компьютеры с особо важной информацией или функциями либо сети, в которых проводятся эксперименты над сетевым оборудованием.

Хорошим примером секретных сетей являются банковские сети. Каждый вечер банки связываются с системой федерального резерва для передачи денежных средств. Ошибки в этих сетях могут стоить банкам больших денег. Системы, управляющие такими соединениями, являются крайне секретными и жизненно важными для банковских структур. Для ограничения доступа к этим системам из других подразделений банка можно установить межсетевой экран.

Рис. 10.5. Архитектура 3: двойные межсетевые экраны

Как видно из таблицы 10-3, правила в данном случае аналогичны правилам межсетевого экрана в архитектуре 2. Но еще имеется и второй межсетевой экран. Правила для межсетевого экрана 2 приведены в табл. 10-4.

Таблица 10.3. Правила межсетевого экрана 1 в архитектуре с двумя межсетевыми экранами

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Любой	Веб-сервер	HTTP	Принятие
2	Любой	Почтовый сервер	SMTP	Принятие
3	Почтовый сервер	Любой	SMTP	Принятие
4	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, telnet, SSH	Принятие
5	Внутренняя DNS	Любой	DNS	Принятие
6	Любой	Любой	Любая	Сброс

Таблица 10.4. Правила межсетевого экрана 2 в архитектуре с двойным межсетевым экраном

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Внутренний почтовый сервер	Почтовый сервер	SMTP	Принятие

2	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, telnet, SSH	Принятие
3	Внутренняя DNS	Любой	DNS	Принятие
4	Любой	Любой	Любая	Сброс

Примечание

Эти примеры очень просты, однако они отражают функционирование межсетевых экранов, при котором разрешается только строго определенный доступ.

Построение набора правил межсетевого экрана

Качественно созданный набор правил не менее важен, чем аппаратная платформа. Большая часть межсетевых экранов работает по принципу "первого соответствия" при принятии решения о передаче или отклонении пакета. При построении набора правил согласно алгоритму "первого соответствия" наиболее специфичные правила располагаются в верхней части набора правил, а наименее специфичные (т. е. более общие) - в нижней части набора. Такое размещение правил гарантирует, что общие правила не перекрывают собой более специфичные.

Примечание

Некоторые межсетевые экраны содержат обработчик набора правил, проверяющий набор на наличие правил, перекрываемых другими правилами. Обработчик информирует об этой ситуации администратора межсетевого экрана перед установкой правил на межсетевой экран.

Данный подход хорош в общем плане, однако он не решает проблему производительности межсетевого экрана. Чем больше правил необходимо проверять для каждого пакета, тем больше вычислений должен производить межсетевой экран. При разработке качественного набора правил следует принимать в расчет это обстоятельства, т. к. от него зависит уровень эффективности работы межсетевого экрана.

Для повышения эффективности работы экрана следует оценить ожидаемую нагрузку трафика на межсетевой экран и упорядочить трафик по типам. Как правило, наибольший объем занимает трафик HTTP. Для повышения эффективности межсетевого экрана следует разместить правила, относящиеся к HTTP, вверху набора правил. Это означает, что правило, позволяющее внутренним системам использовать HTTP для подключения к любой системе в интернете, и правило, разрешающее внешним пользователям осуществлять доступ к веб-сайту организации, должны быть

расположены очень близко к верхней границе набора правил. Единственными правилами, которые должны находиться выше двух упомянутых правил, являются специфичные правила отказа в доступе, относящиеся к протоколу HTTP.

Выявление различий между межсетевыми экранами различных типов

Данный проект продемонстрирует различия в системах защиты межсетевых экранов различных типов. Для выполнения этого проекта необходим доступ к межсетевому экрану прикладного уровня, а также к экрану с фильтрацией пакетов.

Шаг за шагом

1. Сконфигурируйте сеть согласно архитектуре 2. Не подключайте эту сеть к интернету!
2. Создайте почтовый сервер и веб-сервер с настройками по умолчанию и оставьте в каждой системе уязвимости.
3. Разместите межсетевой экран прикладного уровня в сети и настройте его согласно набору правил из табл. 10.2.
4. Сконфигурируйте другую систему в качестве внешней системы (как если бы она располагалась вне межсетевого экрана в интернете) и запустите сканер уязвимостей.
5. С помощью сканера уязвимостей просканируйте почтовый сервер и веб-сервер, а также межсетевой экран.
6. Теперь замените межсетевой экран прикладного уровня межсетевым экраном с фильтрацией пакетов.
7. Снова просканируйте серверы.
8. Сравните полученные результаты. Различна ли информация, полученная при первом и втором сканировании? Одинаковы ли уязвимости, отображенные при подключении обоих межсетевых экранов? Если нет, то почему?

Выводы

Если модули доступа на межсетевом экране прикладного уровня настроены правильно, в результате сканирования через экран с фильтрацией пакетов, скорее всего, отобразится большее число уязвимостей, чем при сканировании через межсетевой экран прикладного уровня. Причиной этому является то, что модуль доступа перехватывает и интерпретирует почту и веб-запросы перед отправкой на серверы. В некоторых случаях этот подход обеспечивает защиту от использования уязвимостей серверов.

Контрольные вопросы

1. Выделите два основных типа межсетевых экранов.

2. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?
3. Является ли один из типов межсетевых экранов более безопасным, нежели другой?
4. Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
5. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?
6. Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией?
7. Что должен обеспечивать межсетевой экран для проверки состояния?
8. При каком условии межсетевой экран прикладного уровня может называться гибридным?
9. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном?
10. Почему порядок правил в наборе правил межсетевого экрана играет важную роль?