51. Системы безопасности. Фильтрация трафика (формальный брандмауэр). Системы обнаружения и предотвращения вторжения. Обобщенная архитектура. Принципы работы.

Существует несколько методов обеспечения информационной безопасности:

- средства идентификации и аутентификации пользователей (так называемый комплекс ЗА);
- средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;
- межсетевые экраны;
- виртуальные частные сети;
- средства контентной фильтрации;
- инструменты проверки целостности содержимого дисков;
- средства антивирусной защиты;
- системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Каждое из перечисленных средств может быть использовано как самостоятельно, так и в интеграции с другими. Это делает возможным создание систем информационной защиты для сетей любой сложности и конфигурации, не зависящих от используемых платформ.
"Комплекс ЗА" включает *аутентификацию* (или идентификацию), *авторизацию* и *администрирование*.

Идентификация и авторизация - это ключевые элементы информационной безопасности. При попытке доступа к информационным активам функция идентификации дает ответ на вопрос: "Кто вы" и "Где вы" - являетесь ли вы авторизованным пользователем сети. Функция авторизации отвечает за то, к каким ресурсам конкретный пользователь имеет доступ. Функция администрирования заключается в наделении пользователя определенными идентификационными особенностями в рамках данной сети и определении объема допустимых для него действий.
Системы шифрования позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам. Задача данного средства защиты - обеспечение конфиденциальности. Основные требования, предъявляемые к системам шифрования - высокий уровень криптостойкости и легальность использования на территории России (или других государств).

Межсетевой экран представляет собой систему или комбинацию систем, образующую между двумя или более сетями защитный барьер, предохраняющий от несанкционированного попадания в сеть или выхода из нее пакетов данных.

Основной принцип действия межсетевых экранов - проверка каждого пакета данных на соответствие входящего и исходящего IP-адреса базе разрешенных адресов. Таким образом, межсетевые экраны значительно расширяют возможности сегментирования информационных сетей и контроля за циркулированием данных.

Говоря о криптографии и межсетевых экранах, следует упомянуть о защищенных **виртуальных частных сетях** (Virtual Private Network - VPN). Их использование позволяет решить проблемы конфиденциальности и целостности данных при их передаче по открытым коммуникационным каналам. Использование VPN можно свести к решению трех основных задач:

- защита информационных потоков между различными офисами компании (шифрование информации производится только на выходе во внешнюю сеть);
- защищенный доступ удаленных пользователей сети к информационным ресурсам компании, как правило, осуществляемый через интернет;
- защита информационных потоков между отдельными приложениями внутри корпоративных сетей (этот аспект также очень важен, поскольку большинство атак осуществляется из внутренних сетей).

Эффективное средство защиты от потери конфиденциальной информации - **фильтрация** содержимого входящей и исходящей электронной почты. Проверка самих почтовых сообщений и вложений в них на основе правил, установленных в организации, позволяет также обезопасить компании от ответственности по судебным искам и защитить их сотрудников от спама. Средства контентной фильтрации позволяют проверять файлы всех распространенных форматов, в том числе сжатые и графические. При этом пропускная способность сети практически не меняется.

Все изменения на рабочей станции или на сервере могут быть отслежены администратором сети или другим авторизованным пользователем благодаря технологии **проверки целостности** содержимого жесткого диска (integrity checking). Это позволяет обнаруживать любые действия с файлами (изменение, удаление или же просто открытие) и идентифицировать активность вирусов, несанкционированный доступ или кражу данных авторизованными пользователями. Контроль осуществляется на основе анализа контрольных сумм файлов (CRC-сумм).

Современные **антивирусные технологии** позволяют выявить практически все уже известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе. Кроме того, разработаны технологии моделирования поведения, позволяющие обнаруживать вновь

программы. Обнаруживаемые объекты могут подвергаться лечению, изолироваться (помещаться в карантин) или удаляться. Защита от вирусов может быть установлена на рабочие станции, файловые и почтовые сервера, межсетевые экраны, работающие под практически любой из распространенных операционных систем (Windows, Unix- и Linux-системы, Novell) на процессорах различных типов.

Фильтры спама значительно уменьшают непроизводительные трудозатраты, связанные с разбором спама, снижают трафик и загрузку серверов, улучшают психологический фон в коллективе и уменьшают риск вовлечения сотрудников компании в мошеннические операции. Кроме того, фильтры спама уменьшают риск заражения новыми вирусами, поскольку сообщения, содержащие вирусы (даже еще не вошедшие в базы антивирусных программ) часто имеют признаки спама и отфильтровываются. Правда, положительный эффект от фильтрации спама может быть перечеркнут, если фильтр наряду с мусорными удаляет или маркирует как спам и полезные сообщения, деловые или личные.

Тот огромный урон, который был нанесен сетям компаний в 2003 году вирусами и хакерскими атаками, - в большой мере следствие слабых мест в используемом программном обеспечении. Определить их можно заблаговременно, не дожидаясь реального нападения, с помощью **систем обнаружения уязвимостей** компьютерных сетей и **анализаторов сетевых атак**. Подобные программные средства безопасно моделируют распространенные атаки и способы вторжения и определяют, что именно хакер может увидеть в сети и как он может использовать ее ресурсы. Для противодействия естественным угрозам информационной безопасности в компании должен быть разработан и реализован набор процедур по предотвращению чрезвычайных ситуаций (например, по обеспечению физической защиты данных от пожара) и минимизации ущерба в том случае, если такая ситуация всё-таки возникнет. Один из основных методов защиты от потери данных - **резервное копирование** с четким соблюдением установленных процедур (регулярность, типы носителей, методы хранения копий и т. д.).

Физическая безопасность

Предотвращение неавторизованного доступа к сетевым ресурсам означает, прежде всего, невозможность физического доступа к компонентам сети - рабочим станциям, серверам, сетевым кабелям и устройствам, и т.п. Когда сетевое соединение выходит за пределы вашей зоны влияния, например в точке подключения к внешнему провайдеру интернета, то контроль за физическими аспектами сети, разумеется, теряется - и остается полагаться на другие методы, такие как шифрование и туннелирование. Но оборудование в помещении компании должно находиться под пристальным наблюдением.

Как бы глупо это ни звучало, но от несанкционированного доступа часто спасает простой дверной замок. Серверы, на которых хранятся важные или уязвимые данные, не должны стоять открыто на столе или в незапертой комнате, куда может зайти кто угодно. Аналогичным образом должны защищаться маршрутизаторы, концентраторы, коммутаторы и другие устройства. Комнаты с компьютерами должны закрываться на замок или находиться под круглосуточным наблюдением. Если кто-то из сотрудников компании работает круглосуточно, то это комнату закрывать не обязательно - но только в том случае, если персонал не дежурит по одному. В идеале доступ в подобные помещения должен контролироваться, например, путем регистрации в журнале.

Резервные носители, такие как ленты или перезаписываемые компакт-диски, должны быть защищены так же, как и исходные данные. Недопустимо хранить резервные копии на сервере или рабочей станции, оставлять картриджи и CD на столе или в незапертом ящике.

Системы безопасности в IP сетях

Современные системы безопасности предлагают все более совершенные методы защиты корпоративных сетей от различных типов угроз. Однако в них не уделяется достаточного внимания таким уязвимым элементам инфраструктуры, как настольные компьютерные системы. Причем обычно недооценивается не только опасная способность враждебных программных кодов мгновенно распространяться по электронной почте, через Интернет и системы совместного использования файлов, но и та роль, которую играют в этом неправильные и неумелые действия конечных пользователей. А ведь в состав корпоративной сети могу входить сотни или даже тысячи ноутбуков и настольных компьютеров, зачастую географически удаленных друг от друга.

Противоречивость современной сферы информационной безопасности состоит в том, что основной упор в ней делается на защиту периметра и внутренней инфраструктуры сети, несмотря на то, что по статистике наиболее уязвимыми узлами корпоративной сети являются рабочие станции и мобильные компьютеры, на которых обрабатывается большой объем конфиденциальной информации и хранится интеллектуальная собственность компании. Именно они - самое критичное место в построении защиты информационных сетей, так как подвержены угрозам, исходящим как извне, так и от легальных пользователей сети.

Фазы жизни

Рассматривая угрозы настольным компьютерным системам, важно понимать, что для того, чтобы какая-либо атака была успешной, она должна пройти три жизненные фазы: проникновение, выполнение, распространение. Проникновение может быть осуществлено различными методами - посредством электронной почты, через Web-браузер, за счет удаленного переполнения буфера памяти и т.п. Выполнение - это запуск злонамеренного кода, уже загруженного вследствие успешно пройденной первой фазы. Распространение означает компрометацию других ресурсов, составляющих объект атаки, или иных узлов сети - как посредством удаленного управления, так и в автономном режиме.

Двухвекторная модель атак

Структуру угроз настольным компьютерным системам можно представить с помощью двухвекторной модели их возникновения - угрозы атак на уровне сети и угрозы атак на уровне приложений. На сетевом уровне угрозу заключают в себе DoS-атаки и Интернет-черви, на уровне приложений - различные вирусы, E-mail-черви, троянские программы, шпионское программное обеспечение и т.д.

Атаки сетевого уровня (network-based attacks) могут протекать без какого-либо участия пользователя. Они становятся возможными из-за наличия уязвимостей в различных сетевых протоколах и службах. Использование данных уязвимостей реализуется посредством прямого взлома и воровства в информационных сетях, распространения сетевых червей, различных атак типа "отказ в облуживании" (DoS-атаки), установки разнообразных программ, результатом действия которых является появление у злоумышленника путей обхода системы защиты (backdoors) и возможности удаленно управлять узлом сети (footholds). Но этим многообразие видов сетевых атак не ограничиваются: есть еще множество различных путей для использования уязвимостей сетевого уровня.

В отличие от сетевых атак, главное орудие атак уровня приложений (application-based attacks), для выполнения которых требуется некоторая форма участия пользователя, - это исполняемые файлы.

Personal Firewall

Персональный межсетевой экран (Personal Firewall, PFW) - наиболее распространенная и понятная форма защиты настольных компьютерных систем для подавляющего числа пользователей. Благодаря набору правил фильтрации пакетов PFW может уменьшить, но не ликвидировать риск того, что компьютер подвергнется нападению из внешней сети. Путем блокирования доступа к портам, IP-адресам, сетевым протоколам и службам PFW-технология может предотвращать только небольшое число хорошо известных атак (SYNFlood, IPSpoofing, Ping of Death, WinNuke и т.д.). Несмотря на свои бесспорные достоинства, технологии межсетевого экранирования не справляются с новыми, постоянно развивающимися угрозами, примерами реализации которых можно назвать известные всем атаки: Nimda, Code Red, Slammer и т.д.

IDS и IPS

Получившая широкое распространение технология обнаружения атак (Intrusion Detection System, IDS) использует глубокий анализ пакетов сетевого трафика, прошедшего через правила фильтрации межсетевого экрана, для извещения пользователя о попытке атаки на информационную систему.

Появившись совсем недавно, технология IDS достаточно быстро переросла в технологию защиты следующего поколения - предотвращение атак (Intrusion Prevention System, IPS). По сути дела, IPS стала результатом объединения функциональных возможностей IDS и систем межсетевого экранирования. Механизм обнаружения атак, как правило, основан на сигнатурных методах анализа пакетов и методах анализа протоколов. Сигнатурные методы (сравнение реального трафика с шаблоном атаки) эффективны для обнаружения уже известных атак и практически беззащитны перед неизвестными атаками.

В свою очередь, методы анализа протоколов обладают потенциалом для обнаружения неизвестных атак и сетевых червей, но имеют недостаток - большое потребление ресурсов при обнаружении атак в реальном времени. Анализ протоколов включает в себя использование целого ряда методик: поведенческого анализа, сравнения структуры и содержания пакетов на соответствие RFC (Request for Comments) и т.д. Предотвращение, в данном случае, возможно только для известных и неизвестных атак, направленных на уже известные уязвимости. Поэтому необходим еще один уровень защиты, предотвращающий атаки на неизвестные уязвимости.

Брандмауэр, файервол, firewall

Учитывая важность проблемы защиты, разработана специальная система **firewall** ("огненная стена" или брандмауэр). Первые Firewall появились в конце 80-х годов, в 1991 году фирма DEC предложила устройство **SEAL** (Secure External Access Link), устройства же современного типа появились в 1993 году (**TIS** – Trusted Information System). Система **firewall** заменяет маршрутизатор или внешний порт сети (gateway). Защищенная часть сети размещается за ним. Пакеты, адресованные Firewall, обрабатываются локально, а не просто переадресуются.

Пакеты же, которые адресованы объектам, расположенным за Firewall, не доставляются. По

вынужден иметь дело с системой защиты ЭВМ Firewall. Схема взаимодействия Firewall с локальной сетью и внешним Интернет показана на рис. 6.3.1.

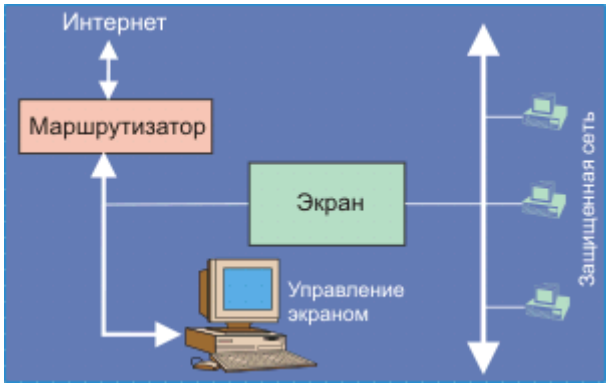

Рис. 6.3.1. Схема Firewall

Такая схема проще и надежнее, так как следует заботиться о защите одной машины, а не многих. Экран, маршрутизатор и ЭВМ управления экраном объединены небольшой, незащищенной локальной сетью. Основные операции по защите осуществляются здесь на IP-уровне. Эту схему можно реализовать и на одной ЭВМ, снабженной двумя интерфейсами. При этом через один интерфейс осуществляется связь с Интернет, а через второй - с защищенной сетью. Такая ЭВМ совмещает функции маршрутизатора-шлюза, экрана и управления экраном. Возможна реализация Firewall, показанная на рис 6.3.2. Здесь функция экрана выполняется маршрутизатором, но и прокси может выполнять некоторые защитные функции. Возможен вариант прокси-сервера и с одним сетевым интерфейсом. Эту схему можно реализовать и на одной ЭВМ, снабженной двумя интерфейсами. При этом через один интерфейс осуществляется связь с Интернет, а через второй - с защищенной сетью.

Рис. 6.3.2. Схема Firewall, где функцию экрана выполняет маршрутизатор

В этой схеме доступ из Интернет возможен только к прокси-серверу, ЭВМ из защищенной сети могут получить доступ к Интернет тоже только через прокси-сервер. Ни один пакет посланный из защищенной ЭВМ не может попасть в Интернет и, аналогично, ни один пакет из Интернет не может попасть непосредственно защищенной ЭВМ. Возможны и другие более изощренные схемы, например со вторым “внутренним” Firewall для защиты от внутренних угроз.

Вне зависимости от того, насколько надежен ваш сетевой экран, не следует снижать требования к безопасному конфигурированию рабочих станций и серверов.

Следует также помнить, что сетевой экран не способен защитить от вирусов, сетевых червей, троянских коней, **атак из локальной сети** и различных мошеннических трюков (“социальная инженерия”). Но самой серьезной угрозой являются “новые” неизвестные доселе атаки. Существует несколько разновидностей Firewall.

Фильтрующие Firewall

Фильтрующая разновидность сетевых экранов производит отбор пакетов по содержимому заголовков (адреса и номера портов). Но такие экраны не могут различить команду get от put, так как для этого надо просматривать поле данных. Функции таких сетевых экранов могут быть реализованы практически любым маршрутизатором.

Прокси Firewall

Сетевые экраны на основе прокси-серверов способны анализировать не только заголовки, но и пересылаемые данные. Такие серверы исключают прямое соединение клиента и удаленного сервера. От имени клиента запрос посылает сетевой экран. Для большой сети целесообразно иметь отдельные машины для прокси-серверов, обеспечивающих разные виды услуг (WWW, FTP и пр.), см. рис. 6.3.3. и 6.3.3А.

Разные серверы для разных услуг помимо безопасности пропорционально увеличивают быстродействие системы в целом.

На рисунках показаны два (но не единственных) варианта защиты сети с помощью сетевого экрана, построенного на основе прокси-сервера и имеющего “демилитаризованную” зону. В такой зоне обычно размещаются серверы, доступные из Интернет непосредственно (вне защищаемого контура). Такие серверы бывают нужны для рекламирования изделий фирмы, обслуживания клиентов или для демонстрации достижений учреждения или научного центра. Такие схемы сохраняют доступность вашего WEB-сервера со стороны поисковых систем, что позволит узнать о вашей компании или учреждении большему количеству людей. Вариант на рис. 6.3.3А несколько гибче, но требует трех сетевых интерфейсов для прокси-сервера. Существуют аппаратные решения, совмещающие многие из описанных здесь возможностей.

Следует помнить, что подключение через модем должно производиться через специальный защищенный сервер с поддержкой протоколов типа Radius. Наилучшее для него место размещения - демилитаризованная зона, ведь безопасность сети определяется ее самым уязвимым элементом.

Рис. 6.3.3. Размещение WEB-сервера в демилитаризованной зоне

При выборе политики и правил отбора пакетов важно ответить на следующие вопросы:

- Какие сетевые услуги вы желаете реализовать и для каких направлений (изнутри и снаружи)?
- Следует ли ограничивать “внутренних” клиентов в части подключения к серверам в Интернет?
- Имеются ли узлы в Интернет, для которых вы бы хотели создать особые условия доступа (например, филиалы вашего учреждения)?

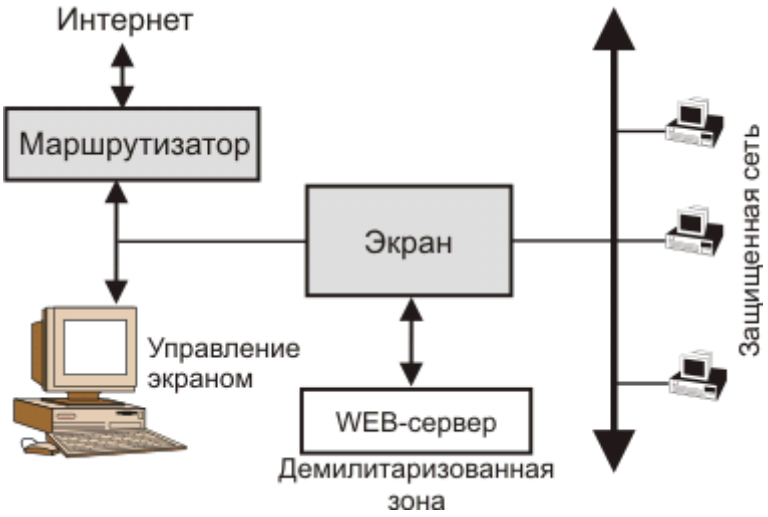

Рис. 6.3.3а. Вариант построения демилитаризованной зоны с помощью сетевого экрана с 3-мя интерфейсами Обычно сетевым экраном реализуется одна из двух политик безопасности:

- Разрешено все, что не запрещено правилами
- Запрещено все, что не разрешено правилами

На первый взгляд может показаться, что эти две политики неотличимы, но это совсем не так. В первом варианте при появлении нового приложения или протокола придется вводить новые ограничительные правила. Второй вариант политики консервативнее и здесь реже приходится менять правила.

Прокси-сервер обычно привязан к конкретному типу приложений и способен разрешать или запрещать выполнение определенных операций. Рассмотрим, как внутренним клиентом через такого рода сервер может быть загружена определенная WEB-страница с сервера в Интернет.

Прямое соединение внутреннего клиента с внешним сервером через сетевой экран невозможно. Прокси-сервер посылает HTTP-запрос внешнему серверу от своего имени с IP-адреса своего внешнего интерфейса, подключенного к Интернет. Понятно, что и отклик от внешнего WEB-сервера придет через указанный интерфейс в прокси-сервер. После получения запрошенной WEB-страницы прокси-сервер производит определенные администратором проверки, после чего открывает сессию передачи полученных данных через свой интерфейс LAN клиенту-заказчику. На фазе проверок возможна сортировка данных и блокировка доступа клиента к определенному типу данных, например, порнографического вида.

Вообще фильтрация данных стала в последнее время широко обсуждаемой проблемой. Отбор может производиться по URL, хотя этот способ селекции мало эффективен, во-первых, потому что URL часто меняются, во-вторых, из-за того, что клиент может всегда заменить URL на IP-адрес. Надежда на то, что в ограничительный список можно включить и IP-адреса, напрасна, так как некоторые программы могут воспринимать IP-адрес в десятичном (а не в десятично-точечном) представлении. Существуют и более изощренные фильтры, где содержимое анализируется по ключевым словам или по характеру вложений (Java или ActiveX).
Выбирая правила фильтрации, нужно сначала сформулировать общую стратегию:

- Какие сервисы в сети нужно обеспечить и в каком направлении (изнутри вовне или извне внутрь).
- Какие ограничения на выход в Интернет для внутренних машин вы готовы установить.
- Имеются ли внешние машины, для которых вы готовы предоставить какие-то формы доступа в вашу сеть.

В разных системах межсетевых экранов правила фильтрации формулируются различным образом, но, как правило, требуются следующие данные:

- В каком направлении и через какой интерфейс передаются пакеты.
- IP-адреса отправителя и получателя
- Допустимые опции IP
- Используемые протоколы высокого уровня (UDP, TCP, ICMP).
- Допустимые типы ICMP-сообщений
- Номера портов отправителя и получателя (для протоколов (UDP и TCP)

Некоторые протоколы желательно отфильтровывать из-за их потенциальной опасности. Работа с ними допускается лишь на специально выделенных машинах.

1. Порт 23 (Telnet), не должен использоваться вообще или использоваться для исследовательских целей на одной ЭВМ
2. Порты 20 и 21 (FTP) лучше закрыть везде, но, в крайнем случае, их можно открыть при необходимости на одном FTP-сервере.
3. Порт 25 (SMTP) обычно разрешается только на центральном почтовом сервере.
4. Порт 53 (DNS) открывается только для серверов имен (первичного и вторичного).
5. Порт 520 (RIP) может быть использован для перенаправления потока данных. Если можно обойтись без протокола маршрутизации RIP, это следует сделать.
6. Порты 70 (Gopher) и 80 (WWW) должны быть открыты только для шлюзов соответствующих приложений.
7. Порт 119 (NNTP -служба новостей) должен использоваться только сервером новостей.
8. Порт 79 (Finger) желательно закрыть, так как через него может быть получена полезная для хакера персональная информация.
9. Порт 69 (TFTP) безоговорочно должен быть закрыт для любых внешних пользователей. Открытие для внутренних пользователей должно осуществляться в случае крайней необходимости для выбранных IP-адресов.
10. Порт 540 (UUCP) лучше заблокировать из-за его уязвимости (сама услуга устарела и ее безопасность не совершенствуется).

В принципе, прокси-серверы могут работать в обоих направлениях, т.е. обеспечивать внешним клиентам доступ к внутренним серверам. Обеспечивая сокрытие данных о клиентах и структуре внутренней сети, прокси-серверы становятся критической точкой системы в целом. Взлом или выход из строя такого устройства может парализовать работу большого числа людей.

Существуют так называемые прозрачные прокси-серверы. Такие серверы создают больший комфорт клиентам, ведь не нужно авторизоваться сначала в прокси или как-то адаптировать свое программное обеспечение. Для клиента создается впечатление, что он работает непосредственно с внешним сетевым объектом, он может даже не знать о существовании прокси. Запросы внутреннего клиента к внешнему серверу перехватываются прокси-сервером и после анализа блокируются или передаются во внешнюю сеть. Пользователь авторизуется на внешнем сервере, а не в прокси. Но у прокси остается возможность блокировки некоторых операций, например, GET или PUT. Прокси может вести журнал операций или предоставлять различные права разным клиентам. Следует заметить, что прозрачный сервер не скрывает IP-адреса внутренних клиентов. Если прокси организует подключение внешнего клиента к внутреннему серверу, для внутреннего сервера клиентом является прокси, а не

внешний объект знает IP-адрес внутреннего сервера. Ситуацию можно несколько улучшить, если поместить все внутренние серверы в демилитаризованную зону, тогда хакер не получит никаких данных об остальных объектах внутренней сети. Внутренние серверы в этом случае должны быть дополнительно защищены, например, локальными программами типа Firewall.

В случае классического прокси клиенту нужно знать имя прокси и ЭВМ, с которой он хочет взаимодействовать. Имя прокси клиент должен преобразовать в его IP-адрес, послав запрос в DNS, а имя ЭВМ передать прокси-серверу в качестве параметра запроса. DNS в этом случае сообщает внутренние IP-адреса только внутренним сетевым объектам. Для работы с внешними IP-адресами служит другой DNS-сервер. В случае же прозрачного прокси схема взаимодействия с DNS идентична той, которая существует при отсутствии сетевого экрана.

Для прокси-серверов достаточно типично использование трансляции сетевых адресов **NAT** (Network Address Translation). Такая схема, среди прочего, позволяет обойтись меньшим числом реальных IP-адресов. При реализации запросов во внешнюю сеть программа NAT подставляет в поле адрес отправителя IP сервера NAT. При получении отклика программа NAT заносит в поле адреса получателя адрес клиента источника запроса. Существуют сетевые услуги, которые следует блокировать сетевым экраном:

- **NFS (Network File System)**. В случае разрешения доступа к этой услуге через сетевой экран, на удаленной машине можно будет смонтировать файловую систему вашей сети и делать с ней все что угодно…
- **NIS** (Network Information System - сетевая информационная система). Эта система позволяет хакерам узнать нужные им имена узлов и пользователей в вашей сети.
- **X-windows**. По уязвимости эта услуга сравнима с Telnet, допускает удаленный запуск процессов.

Не следует оставлять без внимания безобидный на первый взгляд протокол ICMP, так как он позволяет получить много разнообразной и полезной для хакера информации. По этой причине целесообразно блокировать прохождение ICMP-пакетов следующих типов:

- Входящие *echo request* и исходящие *echo replay*. Это сохранит возможность для внутренних клиентов тестировать доступность узлов Интернет, но не даст зондировать ваши внутренние сетевые объекты.
- Входящие сообщения redirect. Такие сообщения позволяют модифицировать таблицу маршрутизации.
- Входящие сообщения service unavailable и исходящие destination unreachable. Это препятствует хакеру зондирование вашей сети. Если хакер может узнать, доступны ли нужные ему узлы или службы, это существенно упростит его задачу.

Если вы поставили и сконфигурировали Firewall, не следует расслабляться. Во-первых, ваш сетевой экран защитит вашу сеть не от всех потенциальных угроз (например, вирусы, сетевые черви, троянские кони, доставляемые по почте, не в его сфере возможностей). Во-вторых, если за экраном не вы один, то вас могут обслужить по части сетевых проблем ваши соседи по локальной сети. По этой причине нужно позаботиться об уязвимости ваших внутренних серверов и рабочих станций.

Расстаньтесь с услугами rlogin, rcp, rexec, telnet (замените на ssh), так как с ними работать удобно не только вам, но и хакерам. По возможности замените услуги FTP на SFTP или scp. Загляните в конфигурационный файл /etc/inetd.conf, а также в /etc/rc.* и удалите все ненужные и потенциально опасные услуги и приложения, например, finger. Не оставляйте без внимания и такие файлы как */etc/networks, /etc/protocols, /etc/services, /etc/hosts*.

Если сетевой экран работает на ЭВМ с ОС Windows, там не должно быть файловой системы FAT, так как она не обеспечивает защиты.

В последнее время появился новый вид услуг - MFWS (Managed Firewall Service). Компании, предоставляющие такую услугу, берутся за настройку и управление сетевыми экранами клиента. Сами сетевые экраны могут располагаться у клиента или сервис-провайдера. О настройке межсетевых экранов смотри firewallbyhand.txt.

Недостатки системы Firewall происходят от ее преимуществ, осложняя доступ извне, система делает трудным и доступ наружу. По этой причине система Firewall должна выполнять функции DNS (сервера имен) для внешнего мира, не выдавая никакой информации об именах или адресах внутренних объектов, функции почтового сервера, поддерживая систему псевдонимов для своих клиентов. Псевдонимы не раскрываются при посылке почтовых сообщений во внешний мир. Служба FTP в системе может и отсутствовать, но если она есть, доступ возможен только в сервер Firewall и из него. Внутренние ЭВМ не могут установить прямую FTP-связь ни с какой ЭВМ из внешнего мира. Процедуры telnet и rlogin возможны только путем входа в сервер Firewall. Ни одна из ЭВМ в защищенной сети не может быть обнаружена с помощью PING (ICMP) извне. И даже внутри сети будут возможны только определенные виды трафика между строго определенными машинами. Понятно, что в целях безопасности защищенная сеть не может иметь выходов во внешний мир помимо системы экран, в том числе и через модемы. Экран конфигурируется так, чтобы маршрут по умолчанию указывал на защищенную сеть. Экран не принимает и не обрабатывает пакеты внутренних протоколов маршрутизации (например, RIP). ЭВМ из защищенной сети может
адресоваться к экрану, но при попытке направить пакет с адресом из внешней сети будет

как маршрут по умолчанию указывает назад в защищенную сеть. Для пользователей защищенной сети создаются специальные входы для FTP/scp, telnet/ssh и других услуг. При этом не вводится каких-либо ограничений по транспортировке файлов в защищенную сеть и блокируется передача любых файлов из этой сети, даже в случае, когда инициатором FTP-сессии является клиент защищенной сети. Единственные протоколы, которым всегда позволен доступ к ЭВМ Firewall являются SMTP (электронная почта) и NNTP (служба новостей). Внешние клиенты Интернет не могут получить доступа ни к одной из защищенных ЭВМ ни через один из протоколов. Если нужно обеспечить доступ внешним пользователям к каким-то данным или услугам, для этого можно использовать сервер, подключенный к незащищенной части сети (или воспользоваться услугами ЭВМ управления экраном, что нежелательно, так как снижает безопасность). ЭВМ управления экраном может быть сконфигурирована так, чтобы не воспринимать внешние (приходящие не из защищенной сети) запросы типа FTP/scp, telnet/ssh и пр., это дополнительно повысит безопасность. Стандартная система защиты здесь часто дополняется программой wrapper. Немалую пользу может оказать и хорошая система регистрации всех сетевых запросов. Системы Firewall часто используются и в корпоративных сетях, где отдельные части сети удалены друг от друга. В этом случае в качестве дополнительной меры безопасности применяется шифрование пакетов. Система Firewall требует специального программного обеспечения. Следует иметь в виду, что сложная и дорогостоящая система Firewall не защитит от “внутренних” злоумышленников. Нужно тщательно продумать систему защиты модемных каналов (сама система Firewall на них не распространяется, так как это не внешняя часть сети, а просто удаленный терминал). Хороший результат можно получить, совместно обрабатывая журнальные файлы IDS и Firewall.

Если требуется дополнительная степень защиты, при авторизации пользователей в защищенной части сети могут использоваться аппаратные средства идентификации, а также шифрование имен и паролей.

В последнее время появилось большое число аппаратных решений для межсетевых экранов. Это, прежде всего CISCO PIX Firewall. Но крайне интересное предложение поступило от компании 3COM (см. www.3com.com/products), где Firewall встроен в сетевой интерфейс и снабжен программным обеспечением, позволяющим мониторировать состояние группы таких интерфейсов.

При выборе той или иной системы Firewall следует учитывать ряд обстоятельств.

1. **Операционная система**. Существуют версии Firewall, работающие с UNIX и Windows NT. Некоторые производители модифицируют ОС с целью усиления безопасности. Выбирать следует ту ОС, которую вы знаете лучше.
2. **Рабочие протоколы**. Все Firewall могут работать с FTP (порт 21), e-mail (порт 25), HTTP (порт 80), NNTP (порт 119), Telnet/ssh (порт 23/22), Gopher (порт 70), SSL (порт 443) и некоторыми другими известными протоколами. Как правило, они не поддерживают SNMP.
3. **Типы фильтров**. Сетевые фильтры, работающие на прикладном уровне прокси-сервера, предоставляют администратору сети возможность контролировать информационные потоки, проходящие через Firewall, но они обладают не слишком высоким быстродействием. Аппаратные решения могут пропускать большие потоки, но они менее гибки. Существует также “схемный” уровень прокси, который рассматривает сетевые пакеты, как черные ящики и определяет, пропускать их или нет. Отбор при этом осуществляется по адресам отправителя, получателя, номерам портов, типам интерфейсов и некоторым полям заголовка пакета.
4. **Система регистрации операций**. Практически все системы Firewall имеют встроенную систему регистрации всех операций. Но здесь бывает важно также наличие средств для обработки файлов с такого рода записями.
5. **Администрирование**. Некоторые системы Firewall снабжены графическими интерфейсами пользователя. Другие используют текстовые конфигурационные файлы. Большинство из них допускают удаленное управление.
6. **Простота**. Хорошая система Firewall должна быть простой. Прокси-сервер (экран) должен иметь понятную структуру и удобную систему проверки. Желательно иметь тексты программ этой части, так как это прибавит ей доверия.
7. **Туннелирование**. Некоторые системы Firewall позволяют организовывать туннели через Интернет для связи с удаленными филиалами фирмы или организации (системы Интранет). Естественно, что информация по этим туннелям передается в зашифрованном виде.

Системы обнаружения и предотвращения вторжения.

Система обнаружения вторжений (**СОВ**) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Соответствующий английский термин — *Intrusion Detection System (IDS)*. Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем. Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которое может нарушить безопасность компьютерной системы. К такой активности относятся

уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей)
Обычно архитектура СОВ включает:

- сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы
- подсистему анализа, предназначенную для выявления атак и подозрительных действий на основе данных сенсоров
- хранилище, обеспечивающее накопление первичных событий и результатов анализа
- консоль управления, позволяющая конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты

Существует несколько способов классифицировать СОВ в зависимости от типа и расположения сенсоров, а также методов, используемых подсистемой анализа для выявления подозрительной активности. Во многих простых СОВ все компоненты реализованы в виде одного модуля или устройства.

Виды систем обнаружения вторжений

В сетевой СОВ, сенсоры расположены на важных для наблюдения точках сети, часто в демилитаризованной зоне, или на границе сети. Сенсор перехватывает весь сетевой трафик и анализирует содержимое каждого пакета на наличие вредоносных компонентов. Протокольные СОВ используются для отслеживания трафика, нарушающего правила определенных протоколов либо синтаксис языка (например, SQL). В хостовых СОВ сенсор обычно является программным агентом, который ведет наблюдение за активностью хоста, на который установлен. Также существуют гибридные версии перечисленных видов СОВ.

- Сетевая СОВ (Network-based IDS, NIDS) отслеживает вторжения, проверяя сетевой трафик и ведет наблюдение за несколькими хостами. Сетевая система обнаружения вторжений получает доступ к сетевому трафику, подключаясь к хабу или свитчу, настроенному на зеркалирование портов, либо сетевое TAP устройство. Примером сетевой СОВ является Snort.
- Основанное на протоколе СОВ (Protocol-based IDS, PIDS) представляет собой систему (либо агента), которая отслеживает и анализирует коммуникационные протоколы со связанными системами или пользователями. Для веб-сервера подобная СОВ обычно ведет наблюдение за HTTP и HTTPS протоколами. При использовании HTTPS СОВ должна располагаться на таком интерфейсе, чтобы просматривать HTTPS пакеты еще до их шифрования и отправки в сеть.
- Основанная на прикладных протоколах СОВ (Application Protocol-based IDS, APIDS) — это система (или агент), которая ведет наблюдение и анализ данных, передаваемых с использованием специфичных для определенных приложений протоколов. Например, на веб-сервере с SQL базой данных СОВ будет отслеживать содержимое SQL команд, передаваемых на сервер.
- Узловая СОВ (Host-based IDS, HIDS) — система (или агент), расположенная на хосте, отслеживающая вторжения, используя анализ системных вызовов, логов приложений, модификаций файлов (исполняемых, файлов паролей, системных баз данных), состояния хоста и прочих источников. Примером является OSSEC.
- Гибридная СОВ совмещает два и более подходов к разработке СОВ. Данные от агентов на хостах комбинируются с сетевой информацией для создания наиболее полного представления о безопасности сети. В качестве примера гибридной СОВ можно привести Prelude.

Пассивные и активные системы обнаружения вторжений

В **пассивной СОВ** при обнаружении нарушения безопасности, информация о нарушении записывается в лог приложения, а также сигналы опасности отправляются на консоль и/или администратору системы по определенному каналу связи. В **активной системе**, также известной как Система Предотвращения Вторжений (IPS — Intrusion Prevention system (англ.)), СОВ ведет ответные действия на нарушение, сбрасывая соединение или перенастраивая межсетевой экран для блокирования трафика от злоумышленника. Ответные действия могут проводиться автоматически либо по команде оператора.

Хотя и СОВ, и межсетевой экран относятся к средствам обеспечения информационной безопасности, межсетевой экран отличается тем, что ограничивает поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и не отслеживает вторжения, происходящие внутри сети. СОВ, напротив, пропускает трафик, анализируя его и сигнализируя при обнаружении подозрительной активности. Обнаружение нарушения безопасности проводится обычно с использованием эвристических правил и анализа сигнатур известных компьютерных атак.

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

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.

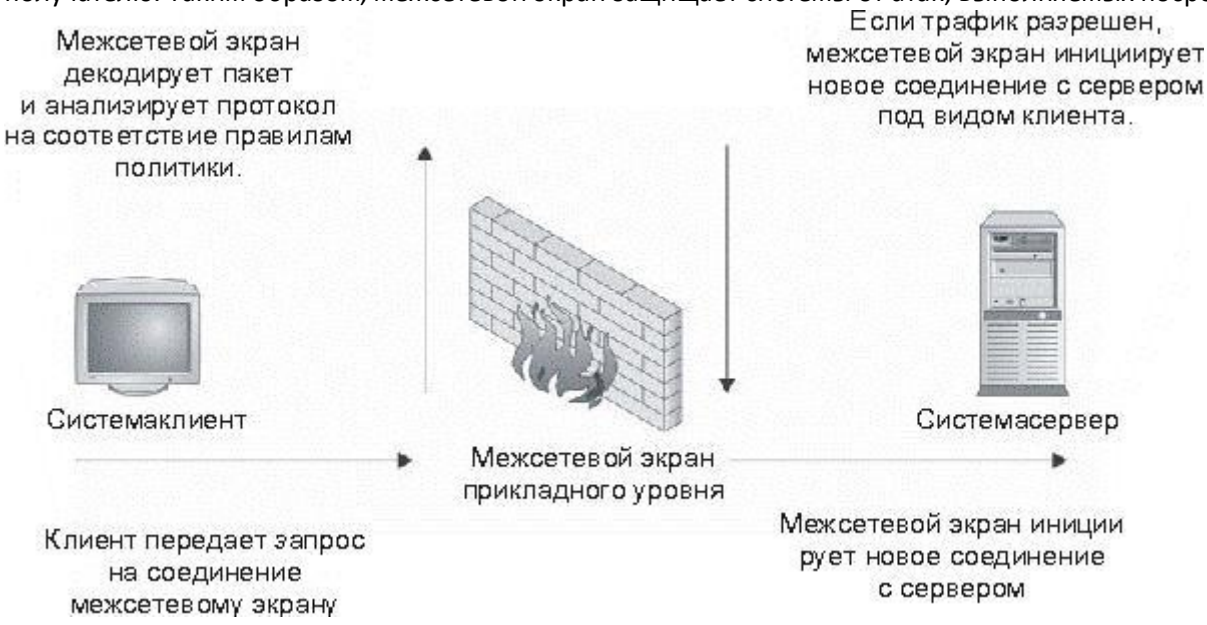

Рис. 10.1. Соединения модуля доступа межсетевого экрана прикладного уровня

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.

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.