Межсетевой экран, аспекты реализации системы защиты

Чем полезен этот материал?

В различных изданиях и публикациях можно найти достаточно много теоретических изысканий, направленных на систематизацию подхода к системе безопасности в существующих компьютерных сетях. Наиболее проработанные материалы, например руководящие документы Государственной Технической Комиссии, стандарты и другие руководящие документы, в основном, ориентированы на оценщиков систем безопасности. Такие документы формулируют необходимые критерии, но практические рекомендации в них, как правило, отсутствуют.

В данной публикации мы попытались соединить воедино теоретическую базу и реальный, накопленный опыт работы с лидирующим на сегодняшний день программным продуктом Check Point FireWall-1.

Почему выбраем Check Point?

Выбор Check Point FireWall-1, как основы для реализации проектов сетевой безопасности, был не случаен. Check Point реализовал в своем продукте совершенно новый подход к инспекции IP пакетов. Метод получил высокую оценку, и Statefull Inspection Technology была запатентована. Многие производители систем firewall используют принципиально похожие технологии. По материалам IDC доля рынка данного продукта на 1997 год составила 44%, что больше, чем доли всех ближайших конкурентов вместе взятых. В России Check Point FireWall-1 начал пользоваться заслуженной популярностью в 1995 году. Появление крупных проектов потребовало должной технической поддержки и, как следствие, необходимости плотно взаимодействовать непосредственно с производителем.

Что такое межсетевой экран?

Теперь немного терминологии. В данной статье мы будем использовать понятия Межсетевой Экран, Брандмауэр, firewall, шлюз с установленным дополнительным программным обеспечением firewall, как эквивалентные. Уточним основные понятия (по материалам Руководящего Документа Государственной Технической Комиссии):

Под сетями ЭВМ, распределенными автоматизированными системами (АС) в данном документе понимаются соединенные каналами связи системы обработки данных, ориентированные на конкретного пользователя.

МЭ представляет собой локальное (однокомпонентное) или функционально - распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Упрощенно, firewall - это устройство, устанавливаемое между сетями и предназначенное для контроля трафика между этими сетями.

Как видно из определения, основное назначение систем firewall – регламентировать использование ресурсов одних сетей пользователями других. Появление таких устройств обусловлено существенным усложнением архитектуры сетей, ростом числа различных сетевых сервисов. Основная идея, положенная в основу этого решения, – сосредоточить в одной критической точке все необходимые контрольные функции вместо того, чтобы контролировать доступ и используемые сервисы на всех компонентах сети. Наиболее широкое распространение эта технология защиты получила при массовом использовании публичных сетей.

Какие бывают угрозы, каковы их последствия, стоимость системы защиты.

Остановимся подробнее на тех опасностях и проблемах, которые подстерегают организацию при работе с подобными сетями, например Интернет.

Существует достаточно много различных аналитических разработок по оценке рисков для подобных сетей. В основном риски сводятся к трем категориям, это:

1. Несанкционированный доступ к ресурсам сети.
2. Нелегальное ознакомление с информацией.
3. Отказ в предоставлении ресурса сети.

Как это ни парадоксально, но для компаний, активно использующих Интернет в повседневной деятельности, влияние третьего фактора риска может быть очень существенным.

Остановимся немного подробнее на рассмотрении угроз, которые могут привести к возникновению перечисленных выше рисков.

Наиболее опасными и, к сожалению, самыми распространенными являются непреднамеренные ошибки операторов информационных систем. Результатом такой ошибки может стать брешь в системе защиты, потеря данных, остановка или выход из строя системы. Один из путей минимизации рисков,

связанных с этим типом угроз – максимальная автоматизация рабочего процесса, контроль за точным соблюдением инструкций и повышение квалификации персонала.

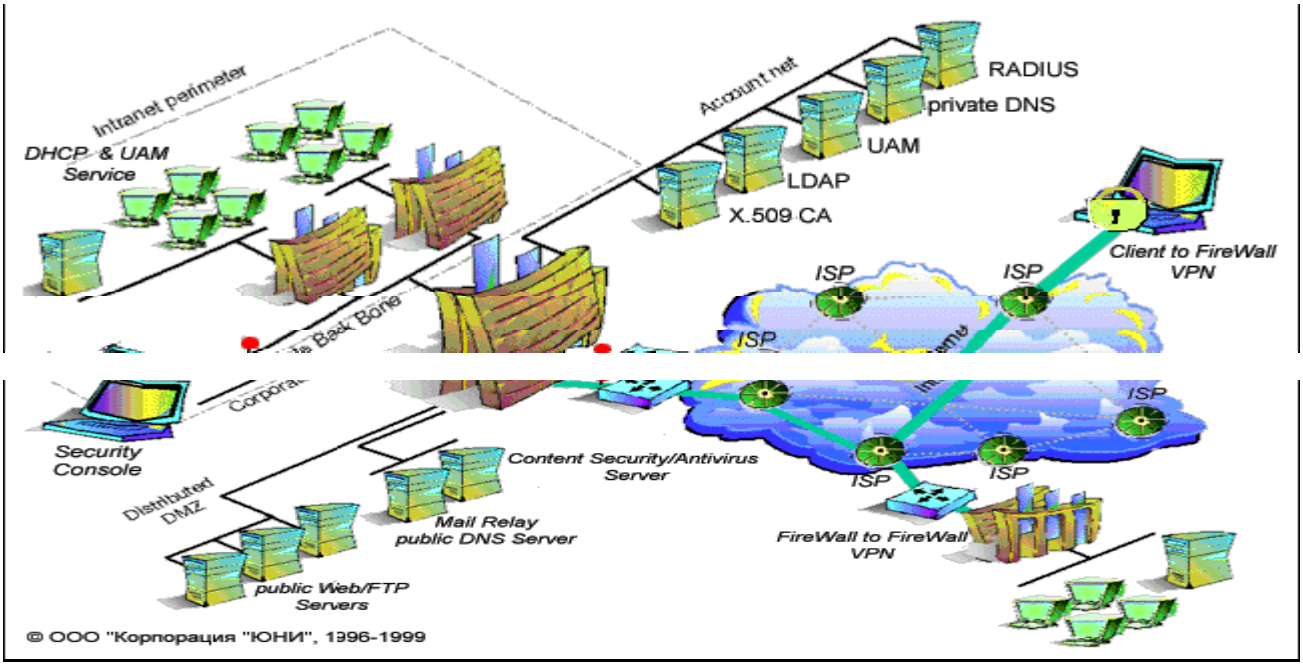
Заметим, что ущерб от краж и подлогов, совершенных с использованием компьютеров находится всего лишь на втором месте. Мы хотим подчеркнуть, что основная опасность исходит непосредственно от персонала предприятия, независимо от того, преднамеренные или непреднамеренные действия создают эту угрозу.

Основное отличие внешних угроз это их непредсказуемость. К внешним угрозам мы относим не только попытки проникновения в сети предприятия с использованием слабостей в реализации той или иной стратеги защиты и администрирования, но и такие "мирные" угрозы, как пропадание электропитания, обрыв информационного кабеля и т.д. По статистике, ущерб, нанесенный хакерами, намного меньше, чем ущерб, связанный с выходом из строя отдельных элементов инфраструктуры.

Далее мы попытаемся дать несколько практических советов по реализации сетевой инфраструктуры, обратим Ваше внимание на некоторые аспекты администрирования системы защиты, которые направлены на минимизацию приведенных выше рисков, на типичном примере реализации системы защиты при доступе к Интернет.

Структура сети и ее вклад в политику защиты.

При построении системы защиты значительное влияние на результативность применяемых мер оказывает правильный выбор структуры сети. Этот фактор обычно сказывается как на облегчении задач разработки политики безопасности и управлении firewall, так и на повышении устойчивости защиты. Во многих случаях, неправильное размещение какого-либо сетевого объекта может создать трудности для контроля некоторых видов трафика и в детектировании попыток взлома сети. Примерная схема сети компании с доступом в Интернет приведена на рисунке.



Данная схема ориентирована, в первую очередь, на компании, реализующие полнофункциональное подключение к Интернет. В некоторых случаях (где часть сервисов предоставляет провайдер) отдельные элементы схемы могут отсутствовать. Практически, реализация данной схемы не зависит от величины компании, важно только наличие или отсутствие соответствующих сетевых сервисов.

Распределенная DMZ и минимизация внутренних угроз.

Одним из примеров решения по выбору структуры сети является размещение публично доступных серверов – Web, FTP, SMTP, DNS в распределенной демилитаризованной зоне. С одной стороны, эти серверы должны быть доступны для всего внешнего мира, с другой -необходимо строго контролировать попытки доступа к ним. В случае достаточно крупной компании, администратору становится почти невозможно контролировать все соединения к этим серверам, так как это заняло бы как минимум весь рабочий день. С другой стороны, именно эта часть системы подвержена наибольшему риску оказаться объектом атаки, как по причине своей очевидной доступности извне, так и из-за массы известных и регулярно обнаруживаемых новых ошибок в реализации программ, обеспечивающих эти типы сервиса. Даже при безупречном программном обеспечении, существуют некоторые возможности прервать работу публичных серверов, используя особенности реализации стека TCP/IP. Так или иначе, даже если

администраторы сети постоянно следят за всеми публикациями об обнаруженных ошибках и устанавливают все выпускаемые "заплатки", нет никакой гарантии, что некто не сможет получить доступ к публичным серверам. Единственной гарантией может служить только полная изоляция.

Вследствие этого, все доступные извне сервера обычно размещают в специально отведенной только для них зоне так, чтобы в худшем случае под угрозой оказался только единственный участок сети. Еще более предпочтительным вариантом является подключение каждого из публичных серверов на отдельный сетевой интерфейс firewall. Это дает как возможность со 100% уверенностью контролировать весь трафик такого сервера, так и защищенность одного публичного сервера от другого в случае нарушения безопасности одного из серверов. То есть даже в случае если кто-то сумел найти ошибку в одной из программ и получить доступ к машине, доступ с этой машины ко всем остальным будет защищен firewall не меньше, чем для любого другого доступа извне. В случае с размещением всех серверов в одной сети такой возможности не существует, и имея доступ к одной из машин, доступ или нарушение работы остальных представляется достаточно простой задачей.

FTP, HTTP-proxy - помощник или конкурент?

Все системы firewall обычно делятся на два основных класса – packet-filtering и application proxy. Системы первого типа свои функции выполняют на уровне протокола TCP/IP. Вторые обычно являются набором программ прокси для каждого из поддерживаемых типов сервисов. Firewall-1 имеет свойства каждого из этих классов и, казалось бы, наличие дополнительного сервера proxy для http и ftp является избыточным. Однако в некоторых случаях такой прокси сервер позволяет сильно упростить политику безопасности, а также закрыть ряд неприятных возможностей доступа извне на машины во внутренних сетях.

Firewall-1 имеет ряд полезных возможностей по контролю за соединениями http и ftp – запрещение доступа к спискам URL, вырезание тегов Java и ActiveX из загружаемых страничек, антивирусная проверка файлов, ограничение доступа по паролю и т.п. Однако такая проверка обычно выполняется для стандартного протокола http, который использует порт 80. Безусловно, существует возможность описания и других портов, но это становится не очень удобным, а иногда такой вариант и просто неприемлем, так как очень многие русскоязычные сайты используют для разных кодировок совершенно произвольные порты. В таком случае приходится либо открывать для доступа наружу все старшие порты TCP/IP, либо постоянно добавлять тот или иной порт для новых сайтов. Кроме того, ряд сайтов использует тот же номер порта, что и доступные http-прокси вне локальной сети предприятия. В случае необходимости применения ограничений на http, такой вариант с внешними прокси сводит на нет все усилия администратора.

Также достаточно неприятным моментом является возможность открытия соединений извне к машинам в локальной сети предприятия с использованием стандартных средств протокола ftp – обратного соединения. В случае если firewall позволяет пользователям работать напрямую по протоколу ftp, для передачи данных обычно используется соединение, открываемое машиной, находящейся вне внутренней сети к машине, запросившей файл. Причем в зависимости от реализации firewall, такое обратное соединение может быть открыто либо только к машине, инициировавшей ftp-сессию (такая проверка есть в Firewall-1), либо вообще к любой машине.

Установка прокси сервера на отдельном сетевом сегменте системы firewall позволяет решить эти проблемы. Так как все пользователи обращаются к прокси серверу по единственному порту TCP, есть возможность применения всех средств контроля протоколов ftp и http в одном месте – между пользователями и прокси сервером. В случае с протоколом ftp, установка прокси исключает возможность использования обратного соединения, так как всю работу по ftp прокси сервер выполняет сам. Заметим, что использование только прокси сервера в качестве центрального элемента защиты во многих случаях просто невозможно.

Служба DNS - двуликий Янус.

При построении системы защиты предприятия, имеющего доступ в публичные сети, важным принципом является сокрытие информации о внутреннем устройстве сети от внешних лиц. Один из источников такой информации – служба имен DNS. Классическим решением этой задачи может служить установка двух отдельных серверов DNS – одного для обслуживания запросов внутренних пользователей, другого для запросов имен извне (некоторые системы защиты предоставляют средства, объединяющие эти два DNS сервера на одном компьютере, но функциональность этих средств, как правило, ограничена). Внутренний сервер должен содержать всю информацию о внутренней сети предприятия, а для разрешения запросов об именах внешних машин обращаться ко внешнему серверу организации. Внешний же сервер имеет только записи, необходимые для поддержания функционирования сервера имен и имена публичных серверов (SMTP, Web, FTP). Такая структура позволяет создать полноценную службу DNS внутри организации и вместе с тем на все внешние запросы DNS сообщать информацию только лишь о доступных всем серверах.

Адресная трансляция.

При подключении к Интернет организация обычно получает в свое использование одну сеть класса С. Это позволяет использовать 254 уникальных адреса для компьютеров в сети предприятия. При использовании внутри сети маршрутизаторов эта цифра еще меньше. Кроме очевидной проблемы с количеством, использование выделенных адресов Интернет достаточно сильно снижает гибкость в распределении адресов, создает массу трудностей при смене провайдера услуг Интернет, обеспечивает потенциальную возможность доступа извне к любой машине, имеющей такой адрес. Не случайно в пространстве IP адресов существуют области, специально зарезервированные для внутреннего использования. При применении этих адресов администратор сети имеет возможность назначать внутренним машинам адреса из сетей любого класса по своему усмотрению. Это снимает все ограничения на количество IP адресов во внутренней сети и вместе и тем затрудняет задачу доступа к таким адресам из внешнего мира. В простейшем случае с помощью NAT (Network Address Translation) возможно организовать работу всей компании с использованием единственного зарегистрированного адреса IP.

Для организации работы с Интернет таких сетей используется механизм трансляции адресов (NAT). Обычно эти функции (NAT) выполняет либо маршрутизатор, используемый для доступа в Интернет, либо система firewall – эти устройства подменяют адреса в заголовках IP пакетов, проходящих через них. Check Point Firewall-1 имеет достаточно гибкие возможности по организации NAT. В простейшем случае администратору достаточно поставить галочку, разрешая трансляцию адресов и указать в какой реальный адрес (или начиная с какого) и как (Static/Hide) транслировать адрес данной машины, сети или набора адресов. Если же требуется более сложная конфигурация, Firewall-1 позволяет в ручном режиме задать правила трансляции адресов в зависимости от адресов источника/назначения и типа протокола, которому принадлежит пакет.

Удаленный доступ в схеме корпорация и провайдер.

Во многих организациях необходимо обеспечить возможность работы удаленных или мобильных пользователей с каким-либо ресурсом внутренней сети компании. Такие пользователи получают доступ либо по телефонной линии через модем, либо через ближайшего к ним провайдера Интернет. Оба случая требуют особого внимания к аутентификации пользователей и защите передаваемых данных. Хорошим решением в таких случаях могут стать средства Firewall-1 SecuRemote. Этот пакет может быть установлен на компьютерах удаленных пользователей для защиты от прослушивания/изменения передачи конфиденциальной информации и процедуры входа/регистрации в сети/аутентификации. Для достижения цели SecuRemote использует средства с открытым ключом. Причем использование этих возможностей может быть ограничено лишь отдельными видами трафика, тогда как остальной обмен (например выход в Интернет) может передаваться в открытом виде. Эта выборочность позволяет значительно сократить требования к вычислительной мощности, как клиента, так и центральной системы firewall. Аутентификация firewall поддерживает целый ряд программных и аппаратных средств третьих производителей – ActiveCard, Axent/AssureNet, Funk Software, Security Dynamics/RSA, VASCO Data Security. При реализации удаленного доступа мы рекомендуем устанавливать устройства удаленного доступа на отдельный интерфейс системы firewall. Как отмечалось выше, это позволяет полностью контролировать как доступ к серверам удаленного доступа, так и все процессы авторизации пользователей (обычно в крупных системах используются внешние серверы авторизации). Также такое решение позволяет использовать механизмы адресной трансляции. В некоторых случаях может потребоваться подключение удаленного клиента с реальным адресом. Однако заметим, что такое расположение сервера удаленного доступа не противоречит этому требованию. Возможности системы FireWall-1 по сбору информации о трафике клиентов позволяют решить проблемы с тарификацией для ISDN подключений.

Схема с полностью скрытым шлюзом (и VPN).

Как бы не была построена сеть компании и система защиты, ключевым местом является сам firewall. Как правило, большинство ограничений и проверок выполняются именно этой машиной, и firewall имеет интерфейсы во все основные сети предприятия. Защита самого firewall по этой причине является одной из важных задач в обеспечении безопасности сети. Два основных элемента используются для решения этой задачи. Первый – это выключение на компьютере всех, не относящихся к firewall служб и запрещение любого трафика адресатом или инициатором которого мог бы быть firewall. Модули Firewall-1 устанавливаются сразу за драйверами сетевых адаптеров, до операционной системы, что позволяет оградить firewall от различных атак, направленных на стек TCP/IP. Вторым шагом, обычно предпринимаемым для затруднения неавторизованного доступа к firewall, является использование адресов из зарезервированного пространства самим firewall. Для попытки подключения к такой машине, во-первых, необходимо узнать ее IP адрес, что практически невозможно без доступа к ближайшим к firewall

маршрутизаторам. Если такой адрес все же стал известен, определенные усилия требуются для доставки пакета с таким "нелегальным" адресом назначения через публичную сеть.

Организация такой схемы защиты требует наличия маршрутизатора между firewall и внешней сетью. Это устройство необходимо для использования зарезервированных адресов на всех интерфейсах firewall, а также для фильтрации нежелательных пакетов с внешнего интерфейса firewall. Конечно, необходимо обеспечить защиту внешнего маршрутизатора, но эта задача несоизмеримо проще. Как правило, предоставляемые маршрутизаторами средства фильтрации прекрасно приспособлены для задачи защиты самого устройства и в меньшей степени пригодны для реализации полнофункциональной защиты предприятия. Для облегчения задачи создания правил фильтрации можно использовать Firewall-1 Router Extension, который поддерживает генерацию и установку списков фильтрации на маршрутизаторы Bay Networks, Cisco, 3Com. Этот механизм полностью интегрирован в политику безопасности Firewall-1 и его средства управления и мониторинга.

Протоколы администрирования сетевых устройств.

Большинство сетевых устройств управляется и конфигурируется либо по протоколу telnet, либо SNMP v1, причем многие не имеют возможности задания списка адресов станций управления. Авторизация построена на передаче секретной строки текста, причем эта передача идет в незакодированном виде. Таким образом, любой пользователь, находящийся в одном сегменте с администратором потенциально способен узнать полную конфигурацию или даже получить доступ к управлению устройствами. При построении системы защиты имеет смысл постараться привести структуру сети к такому виду, чтобы возможность таких действий была сведена к минимуму. Одним из решений, не требующих замены или модернизации сетевых устройств для поддержки какого-либо из протоколов с защитой информации, является вынесение всех администраторов и интерфейсов сетевых устройств, через которые ведется управление, в одну сеть или в одну виртуальную локальную сеть. Связь выделенной для управления части сети с остальными частями внутренней сети и внешним миром должна быть защищена firewall с блокировкой всего SNMP, telnet и др. трафика в направлении этой сети.

Вирусы в сети и способы борьбы с ними.

Кроме стандартных способов борьбы с вирусами – сканированием дисковых разделов, где хранятся файлы и почтовых ящиков, в Firewall-1 имеется возможность проводить проверку всего входящего и выходящего SMTP, FTP и HTTP трафика на наличие в нем вирусов и архивов с зараженными файлами. Специально для этих целей создан протокол CVP (Content Vectoring Protocol). Многие компании-изготовители антивирусных средств имеют продукты, поддерживающие этот протокол (Symantec, EliaShim, McAfee, Integralis, Cheynne). Такой антивирусный сервер представляет собой отдельный компьютер с работающим на нем антивирусным программным обеспечением. Firewall передает этому серверу все проходящие через него файлы, а проверенные или вылеченные передает далее пользователю.

Статья подготовлена по материалам сайта корпорации Юни (http://www.uni.ru/)

За дополнительной информацией Вы можете обращаться к менеджерам компании «Кредиткард».
г.Ростов-на-Дону,
ул. Текучева, 187
тел.: (8632) 64-94-66, 64-93-33
факс.: (8632) 64-47-33
E-mail: info@ccard.ru
http://www.ccard.ru