Содержание:

ВВЕДЕНИЕ

Так необходимая всем всемирная глобальная сеть Internet далеко не безопасное место. Через интернет мошенники активно распространяют откровенно вредоносные либо зараженные, с виду безобидные программы. Каждый может нарваться на такой неприятный сюрприз, следствием которого является утечка личной информации и снятие средств с банковских счетов, злоумышленное шифрование данных, повреждение системных файлов и нарушение работы компьютера. Барьером для всех вышеперечисленных угроз выступает брандмауэр Windows.

Internet, как и любое сообщество, страдает от пользователей, получающих удовольствие от электронной разновидности похабной писанины на стенах, поджигания почтовых ящиков или гудения автомобильными сигналами во дворах. Многие пытаются сделать с помощью сети Internet что-то полезное, у других есть важные или конфиденциальные данные, требующие защиты. Обычно задача брандмауэра – оградить сеть от недобросовестных пользователей, не мешая при этом выполнению работы.

Многие традиционные компании и центры обработки данных разработали правила и принципы компьютерной безопасности, которым надо следовать. Если правила работы компании указывают, как необходимо защищать данные, брандмауэр становится особенно важным, становясь частью корпоративной системы безопасности. Зачастую при подключении большой компании к сети Internet самым трудным является не обоснование того, что это выгодно или полезно, а объяснение руководству, что это вполне безопасно. Брандмауэр не только обеспечивает реальную защиту, он часто играет существенную роль гаранта безопасности для руководства.

Наконец, брандмауэр может служить корпоративным «посланником» («лицом») в Internet. Многие компании используют системы брандмауэров для предоставления широкой общественности информации о продукции и услугах компании, в качестве хранилища файлов для загрузки, источника исправленных версий программ и т.д. Некоторые из этих систем стали важной составляющей спектра услуг сети Internet

(например, UUnet.uu.net, whitehouse.gov, gatekeeper.dec.com), что положительно сказалось на имидже их организаторов.

Некоторые брандмауэры пропускают только сообщения электронной почты, тем самым защищая сеть от любых атак, кроме атак на почтовую службу. Другие брандмауэры обеспечивают менее строгую защиту и блокируют лишь службы, определенно угрожающие безопасности.

Обычно брандмауэры конфигурируются для защиты от неавторизованной интерактивной регистрации из «внешнего» мира. Именно это, больше, чем все остальное, помогает предотвратить проникновение вандалов в машины сети. Более развитые брандмауэры блокируют передачу информации извне в защищаемую сеть, разрешая при этом внутренним пользователям свободно взаимодействовать с внешним миром. При правильной настройке брандмауэр может защитить от любого типа сетевой атаки.

Таким образом, так как вопросы информационной безопасности в XXI веке играют очень важную роль, то выбранная тема данной работы безусловно является актуальной для рассмотрения.

Вопросами касающимися изучения процессора персонального компьютера занимались такие ученые как Артамонова Н.В., Астахова И.Ф., Баула В. Г., Иртегов Д.В., Коньков К.А., Мартемьянов Ю.Ф., Назаров С.В., Стащук П.В., Тюрин И.В. и др.

Цель работы – рассмотреть назначение, специфику настройки и принцип использования брандмауэра.

Объектом исследования является брандмауэр.

Предметом исследования является назначение, специфика настройки и принцип использования брандмауэра.

Для достижения поставленной цели, в работе будут решены следующие задачи:

– рассмотреть предпосылки использования и сущность брандмауэра;

– определить виды брандмауэров и дать им характеристику;

– рассмотреть функциональные требования и компоненты межсетевых экранов;

– рассмотреть шлюзы сетевого уровня;

– рассмотреть возможности усиленной защиты и аутентификации;

– рассмотреть возможности и ограничения межсетевых экранов.

Структура работы состоит из введения, двух глав, заключения и списка использованных источников.

1. Сущность, виды и возможности брандмауэра

1.1. Предпосылки использования и сущность брандмауэра

Интернет является источником полезной и интересной информации. Но Всемирная паутина может быть довольно опасной: постоянно слышно о взломах корпоративных сетей и о краже банковских счетов. Неплохой преградой на пути хакеров являются брандмауэры – программы, которые блокируют несанкционированную передачу информации по Сети и препятствуют запуску вредоносных программ.

Мало кто сегодня не слышал об угрозах, существующих в виртуальном пространстве. Пока еще остается непреложным тот факт, что компьютер, подсоединенный к сети Интернет, может подвергнуться реальным атакам. К сожалению, нередко встречаются неадекватные или незаконопослушные люди (часто в одном лице), патологически не способные существовать без того, чтобы не портить жизнь другим. Тех из них, которые разбираются в компьютерах и знают, как получить удаленный доступ к файлам, называют хакерами. Чтобы защититься от них, прежде всего нужен хороший брандмауэр [11].

Перечислим основные опасности, существующие в Сети:

1. Приложения-нарушители могут поселиться и запускаться на компьютере незаметно (например, ActiveX или Java-аплеты, внедренные в web-страницу). Эти приложения могут выполнить любую операцию на компьютере, в том числе переслать файлы с частной информацией другим компьютерам или вообще удалить данные из системы;

2. При неправильной настройке системы другие компьютеры могут получить доступ к файлам напрямую, без загрузки специального программного обеспечения;

3. Некоторые виды информации (cookies или referrers) могут быть размещены на компьютере таким образом, что заинтересованные лица могут следить за действиями в Сети и будут знать об интересах;

4. Троянские кони также представляют угрозу компьютеру. Троянцы – это программы, используемые хакерами, которые раскрывают частную информацию (пароли, реквизиты, номера кредитных карт). Одно из главных различий между троянцем и вирусом – это то, что вирус действует на компьютере автономно, а троянский конь напрямую управляется взломщиком из Сети;

5. Интернет-черви обычно проникают в компьютер вместе с почтой, в виде вложений. Некоторые почтовые программы открывают вложения самостоятельно. Неопытные пользователи, не осознавая угрозы, открывают вложения сами. Если открыть такое послание хотя бы один раз, то выполняющийся червь начнет стремительно поражать систему.

6. Масса ненужного трафика в виде баннеров и сообщений снижает пропускную способность компьютера. Хотя эти объекты не могут нанести прямой вред данным, они значительно замедляют скорость соединения;

7. Шпионские программы во многом похожи на троянцев. Они собирают сведения об интересах (посещаемые сайты, установленное программное обеспечение и т.д.) без ведома и согласия.

В настоящее время большинство локальных вычислительных сетей (ЛВС) подключено к сети Интернет. Однако отсутствие эффективных средств защиты информации в существующих сетевых протоколах приводит к различным нарушениям целостности передаваемых данных. Поэтому расширение спектра и повышение требований к уровню конфиденциальности сетевых приложений обусловливает необходимость использования специальных технических средств для разграничения доступа к информационным ресурсам и контроля обмена данными между различными компьютерными сетями.

В качестве таких средств защиты широко применяются межсетевые экраны, называемые в англоязычной литературе firewall.

Брандмауэр (межсетевой экран) – это система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения информации из одной части в другую. Брандмауэры представляют собой целый класс систем, порой сопоставимых по сложности с операционной системой [11].

В другом источнике, дано следующее определение: Брандмауэр, или межсетевой экран – это «полупроницаемая мембрана», которая располагается между защищаемым внутренним сегментом сети и внешней сетью или другими сегментами сети Internet и контролирует все информационные потоки во внутренний сегмент и из него. Контроль трафика состоит в его фильтрации, то есть в выборочном пропускании через экран, а иногда и с выполнением специальных преобразований и формированием извещений для отправителя, если его данным в пропуске отказано. Фильтрация осуществляется на основании набора условий, предварительно загруженных в брандмауэр и отражающих концепцию информационной безопасности корпорации [1].

Идеальный персональный брандмауэр должен выполнять шесть функций [11]:

1. Блокировка внешних атак. В идеале брандмауэр должен блокировать все известные типы атак, включая сканирование портов, IP-спуффинг, DoS и DDoS, подбор паролей и пр.

2. Блокировка утечки информации. Даже если вредоносный код проник в компьютер (не обязательно через сеть, а, например, в виде вируса на купленном пиратском CD), брандмауэр должен предотвратить утечку информации, заблокировав вирусу выход в сеть.

3. Контроль приложений. Неизбежное наличие открытых дверей (то есть открытых портов) является одним из самых узких мест в блокировке утечки информации, а один из самых надежных способов воспрепятствовать проникновению вирусов через эти двери – контроль приложений, запрашивающих разрешение на доступ. Кроме банальной проверки по имени файла, весьма желательна проверка аутентичности приложения.

4. Поддержка зональной защиты. Работа в локальной сети часто подразумевает практически полное доверие к локальному контенту, что открывает уникальные возможности по использованию новейших (как правило, потенциально опасных) технологий. В то же время уровень доверия к Интернет-контенту значительно ниже, а значит, необходим дифференцированный подход к анализу опасности того

или иного содержания.

5. Протоколирование и предупреждение. Брандмауэр должен собирать лишь необходимый объем информации – избыток (равно как и недостаток) сведений недопустим. Возможность настройки файлов регистрации и указания причин для привлечения внимания пользователя весьма приветствуются.

6. Максимально прозрачная работа. Эффективность и применяемость системы часто обратно пропорциональны сложности ее настройки, администрирования и сопровождения. Несмотря на традиционный скепсис в отношении мастеров (wizards) по настройке и прочих «буржуйских штучек», даже опытные администраторы не пренебрегают ими просто в целях экономии времени.

Сетевой экран функционирует как пограничный блокпост, который пропускает трафик и в соответствии со списком правил не дает проникнуть в систему запрещенной информации. Если в систему пытается попасть вирус или вредоносная программа, пользователь увидит окно с оповещением об опасности, например: «Обнаружены программы, которые могут нарушить конфиденциальность или причинить вред». Это значит, что файрвол заподозрил опасность. В окошке будет ее описание, название программы. Это может быть троян, например, Trojan:WIN32/Vundo.MF. В случае подобной опасности нужно удалить вирус и очистить систему, выбрав соответствующие действия в окошке [16].

Файрвол может оповестить и о попытке доступа к сети. Всплывает окошко с надписью «Брандмауэр обнаружил попытку доступа к сети». Если это не действие системной службы или известной неопасной программы (можно проверить ее), нужно заблокировать и проверить систему антивирусом.

Если какая-то программа хочет получить доступ к Интернету, межсетевой экран может оповестить о том, что заблокировал ее некоторые возможности. Если это было запланировано пользователем, в окошке нажать «Разрешить доступ». Так ни одна программа не сможет подключиться к сети без ведома владельца.

Далее рассмотрим виды брандмауэров.

1.2. Виды брандмауэров

Брандмауэры можно классифицировать по следующим критериям:

– по исполнению: программные, аппаратные и смешанного типа (аппаратно-программного);

– по компонентной модели: локальные (работающие на одном хосте) и распределенные (distributed firewall);

– по уровню, на котором функционируют брандмауэры: пакетный, прикладной, уровень соединения.

Аппаратный брандмауэр представляет собой устройство, физически подключаемое к сети. Это устройство отслеживает все аспекты входящего и исходящего обмена данными, а также проверяет адреса источника и назначения каждого обрабатываемого сообщения. Это обеспечивает безопасность, помогая предотвратить нежелательные проникновения в сеть или на компьютер. Программный брандмауэр выполняет те же функции, используя не внешнее устройство, а установленную на компьютере программу [9].

На одном и том же компьютере могут использоваться как аппаратные, так и программные брандмауэры.

Разбивка на уровни является условной, что подразумевает возможность работы отдельно взятого брандмауэра более чем на одном уровне одновременно. Можно сказать, что практически все современные брандмауэры функционируют сразу на нескольких уровнях, стремясь расширить свою функциональность и максимально использовать преимущества работы по той или иной схеме. Такая технология получила название Stateful Inspection, а брандмауэры, работающие по смешанной схеме, называются Stateful Inspection Firewall.

Рассмотрим каждый уровень отдельно:

1. Пакетный уровень

Работа на пакетном уровне заключается в фильтрации пакетов. Решение о том, пропускать данный пакет или нет, принимается на основе следующей информации: IP-адреса, номера портов отправителя и получателя, флаги. По сути, задача администратора сводится к составлению простенькой таблицы, на основании которой осуществляется фильтрация.

Преимущества пакетного уровня:

– низкая стоимость;

– высокая производительность.

Недостатки:

– сложность конфигурирования и поддержки;

– отсутствие дополнительных возможностей;

– рухнувшая сеть остается открытой, то есть незащищенной;

– не защищены от фальсификации IP- и DNS-адреса.

2. Прикладной уровень

Фильтрация на уровне пакетов, конечно, очень проста, но часто ее бывает недостаточно. Информации сетевого и транспортного уровня модели OSI иногда не хватает для эффективной работы, что обусловливает существование систем, работающих на самом верхнем уровне – прикладном. Фактически брандмауэры данного уровня предоставляют собой несколько отдельных подсистем (так называемых application gateways – серверов прикладного уровня), по числу обслуживаемых сервисов. Между пользовательским процессом и нужным сервисом возникает посредник, пропускающий через себя весь трафик и принимающий в рамках установленной политики безопасности решение о его легитимности.

Как правило, современные брандмауэры поддерживают практически весь спектр существующих сервисов: HTTP, FTP, SMTP, POP3, IMAP, Telnet, Gopher, Wais, Finger, News, позволяя либо полностью заблокировать тот или иной сервис, либо ввести некоторые ограничения.

Такая схема работы обеспечивает ряд дополнительных возможностей в области безопасности: во-первых, маскируется структура защищаемой сети; во-вторых, появляется возможность более гибко управлять доступом, например через предоставление разных прав отдельным категориям пользователей и т.д.

Преимущества прикладного уровня:

– маскировка защищаемой сети;

– широкие возможности (строгая аутентификация, детальное протоколирование);

– рухнувшая сеть остается заблокированной, то есть защищенной.

Недостатки:

– высокая стоимость;

– низкая производительность.

3. Уровень соединения

Шлюз на уровне соединения представляет собой систему, транслирующую соединения вовне. При установлении доступа пользовательский процесс соединяется с брандмауэром, который, в свою очередь, самостоятельно устанавливает соединение с внешним узлом. Во время работы брандмауэр просто копирует входящую/исходящую информацию. По большому счету, данный шлюз надо рассматривать не как самостоятельный и самодостаточный механизм, а лишь как специфическое решение некоторых задач, например, для работы с нестандартными протоколами, если необходимо создать систему сбора статистики для какого-то необычного сервиса, предоставить доступ только к определенным внешним адресам, осуществить базовый мониторинг и т. д.

К сожалению, уже существуют системы, специально предназначенные для обхода такого рода ограничений. Примером может служить программный комплекс AntiFirewall от iNetPrivacy Software. Он позволяет общаться посредством ICQ или IRC, использовать FTP и Usenet, забирать почту с внешних серверов POP3 и IMAP (возможность отправки не предоставляется). Способ обхода незатейлив: трафик туннелируется в протокол HTTP (который, как правило, не блокируется), а конвертация происходит на внешних прокси-серверах, которые устанавливают соединения с необходимыми службами по соответствующим протоколам. Такая схема дополнительно предоставляет следующую возможность: IP-адрес пользователя маскируется, обеспечивая определенную анонимность.

2. Использование и настройка брандмауэра

2.1. Функциональные требования и компоненты межсетевых экранов

Функциональные требования к межсетевым экранам включают:

– требования к фильтрации на сетевом уровне;

– требования к фильтрации на прикладном уровне;

– требования по настройке правил фильтрации и администрированию;

– требования к средствам сетевой аутентификации;

– требования по внедрению журналов и учету.

Большинство компонентов межсетевых экранов можно отнести к одной из трех категорий:

– фильтрующие маршрутизаторы;

– шлюзы сетевого уровня;

– шлюзы прикладного уровня.

Эти категории можно рассматривать как базовые компоненты реальных межсетевых экранов. Лишь немногие межсетевые экраны включают только одну из перечисленных категорий. Тем не менее, эти категории отражают ключевые возможности, отличающие межсетевые экраны друг от друга [7].

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящее и исходящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP- заголовках пакетов.

Фильтрующие маршрутизаторы обычно может фильтровать IP-пакет на основе группы следующих полей заголовка пакета:

– IP- адрес отправителя (адрес системы, которая послала пакет);

– IP-адрес получателя (адрес системы, которая принимает пакет);

– порт отправителя (порт соединения в системе отправителя);

– порт получателя (порт соединения в системе получателя);

Порт – это программное понятие, которое используется клиентом или сервером для посылки или приема сообщений; порт идентифицируется 16 – битовым числом.

В настоящее время не все фильтрующие маршрутизаторы фильтруют пакеты по TCP/UDP – порт отправителя, однако многие производители маршрутизаторов начали обеспечивать такую возможность. Некоторые маршрутизаторы проверяют, с какого сетевого интерфейса маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации [5].

Фильтрация может быть реализована различным образом для блокирования соединений с определенными хост - компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех хост-компьютеров и сетей. которые считаются враждебными или ненадежными.

Добавление фильтрации по портам TCP и UDP к фильтрации по IP-адресам обеспечивает большую гибкость. Известно, что такие серверы, как домен TELNET, обычно связаны с конкретными портами (например, порт 23 протокола TELNET). Если межсетевой экран может блокировать соединения TCP или UDP с определенными портами или от них, то можно реализовать политику безопасности, при которой некоторые виды соединений устанавливаются только с конкретными хост - компьютерами.

К положительным качествам фильтрующих маршрутизаторов следует отнести:

– сравнительно невысокую стоимость;

– гибкость в определении правил фильтрации;

– небольшую задержку при прохождении пакетов.

Недостатками фильтрующих маршрутизаторов являются:

– внутренняя сеть видна (маршрутизируется) из сети Internet правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;

– при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;

– аутентификацию с использованием IP-адреса можно обмануть путем подмены IP-адреса (атакующая система выдает себя за другую, используя ее IP-адрес);

– отсутствует аутентификация на пользовательском уровне.

2.2. Шлюзы сетевого уровня

Шлюз сетевого уровня иногда называют системой трансляции сетевых адресов или шлюзом сеансового уровня модели OSI. Такой шлюз исключает, прямое взаимодействие между авторизированным клиентом и внешним хост-компьютером. Шлюз сетевого уровня принимает запрос доверенного клиента на конкретные услуги, и после проверки допустимости запрошенного сеанса устанавливает соединение с внешним хост – компьютером [4].

После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Шлюз следит за подтверждением (квитированием) связи между авторизированным клиентом и внешним хост - компьютером, определяя, является ли запрашиваемый сеанс связи допустимым.

Фактически большинство шлюзов сетевого уровня не являются самостоятельными продуктами, а поставляются в комплекте со шлюзами прикладного уровня. Примерами таких шлюзов являются Gauntlet Internet Firewall компании Trusted Information Systems, Alta Vista Firewall компании DEC и ANS Interlock компании ANS. Например, Alta Vista Firewall использует канальные посредники прикладного уровня для каждой из шести служб TCP/IP, к которым относятся, в частности, FTP, HTTP (Hyper Text Transport Protocol) и Telnet.

Кроме того, межсетевой экран компании DEC обеспечивает шлюз сетевого уровня, поддерживающий другие общедоступные службы TCP/IP, такие как Gopher и SMTP, для которых межсетевой экран не предоставляет посредников прикладного уровня.

Шлюз сетевого уровня выполняет еще одну важную функцию защиты: он используется в качестве сервера-посредника. Этот сервер-посредник выполняет процедуру трансляции адресов, при которой происходит преобразование внутренних IP-адресов в один "надежный" IP-адрес. Этот адрес ассоциируется с межсетевым экраном, из которого передаются все исходящие пакеты. В результате в сети со шлюзом сетевого уровня все исходящие пакеты оказываются отправленными из этого шлюза, что исключает прямой контакт между внутренней (авторизированной) сетью и потенциально опасной внешней сетью. IP-адрес шлюза сетевого уровня становится единственно активным IP-адресом, который попадает

во внешнюю сеть. Таким образом, шлюз сетевого уровня и другие серверы-посредники защищают внутренние сети от нападений типа подмены адресов.

Для устранения ряда недостатков, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать дополнительные программные средства для фильтрации сообщений сервисов типа TELNET и FTP. Такие программные средства называются полномочными серверами (серверами-посредниками),а хост-компьютер, на котором они выполняются, -шлюзом прикладного уровня.

Шлюз прикладного уровня исключает прямое взаимодействие между авторизированным клиентом и внешним хост - компьютером. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне. Связанные с приложением серверы – посредники перенаправляют через шлюз информацию, генерируемую конкретными серверами.

Для достижения более высокого уровня безопасности и гибкости шлюзы прикладного уровня и фильтрующие маршрутизаторы могут быть объединены в одном межсетевом экране. В качестве примера рассмотрю сеть, в которой с помощью фильтрующего маршрутизатора блокируются входящие соединения TELNET и FTP. Этот маршрутизатор допускает прохождение пакетов TELNET или FTP только к одному хост - компьютеру - шлюзу прикладного уровня TELNET/FTP. Внешний пользователь, который хочет соединиться с некоторой системой в сети, должен сначала соединиться со шлюзом прикладного уровня, а затем уже с нужным внутренним хост- компьютером [6].

В дополнение к фильтрации пакетов многие шлюзы прикладного уровня регистрируют все выполняемые сервером действия и, что особенно важно, предупреждают сетевого администратора о возможных нарушениях защиты. Например, при попытках проникновения в сеть извне BorderWare Firewall Server компании Secure Computing позволяет фиксировать адреса отправителя и получателя пакетов, время, в которое эти попытки были предприняты, и используемый протокол. Межсетевой экран Black Hole компании Milkyway Networks регистрирует все действия сервера и предупреждает администратора о возможных нарушениях, посылая ему сообщение по электронной почте или на пейджер. Аналогичные функции выполняют и ряд других шлюзов прикладного уровня.

Шлюзы прикладного уровня позволяют обеспечить наиболее высокий уровень защиты, поскольку взаимодействие с внешним миром реализуется через

небольшое число прикладных полномочных программ-посредников, полностью контролирующих весь входящий и выходящий трафик.

Шлюзы прикладного уровня имеют ряд преимуществ по сравнению с обычным режимом, при котором прикладной трафик пропускается непосредственно к внутренним хост – компьютерам. Их преимущества:

– невидимость структуры защищаемой сети из глобальной сети Internet. Имена внутренних систем можно не сообщать внешним системам через DNS, поскольку шлюз прикладного уровня может быть единственным хост - компьютером, имя которого должно быть известно внешним системам;

– надежная аутентификация и регистрация. Прикладной трафик может быть аутентифицирован, прежде чем он достигнет внутренних хост-компьютеров, и может быть зарегистрирован более эффективно, чем с помощью стандартной регистрации;

– оптимальное соотношение между ценой и эффективностью. Дополнительные или аппаратные средства для аутентификации или регистрации нужно устанавливать только на шлюзе прикладного уровня;

– простые правила фильтрации. Правила на фильтрующем маршрутизаторе оказываются менее сложными, чем они были бы, если бы маршрутизатор сам фильтровал прикладной трафик и отправлял его большому числу внутренних систем. Маршрутизатор должен пропускать прикладной трафик, предназначенный только для шлюза прикладного уровня, и блокировать весь остальной трафик;

– возможность организации большого числа проверок. Защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, что снижает вероятность взлома с использованием "дыр" в программном обеспечении.

К недостаткам шлюзов прикладного уровня относятся:

– более низкая производительность по сравнению с фильтрующими маршрутизаторами; в частности, при использовании клиент-серверных протоколов, таких как TELNET, требуется двух шаговая процедура для входных и выходных соединений;

– более высокая стоимость по сравнению с фильтрующим маршрутизатором.

Помимо TELNET и FTP шлюзы прикладного уровня обычно используются для электронной почты, Windows и некоторых других служб.

2.3. Усиленная защита и аутентификация

Одним из важных компонентов концепции межсетевых экранов является аутентификация (проверка подлинности пользователя). Прежде чем пользователю будет предоставлено право воспользоваться тем или иным сервисом, необходимо убедиться, что он действительно тот, за кого себя выдает. Одним из способов аутентификации является использование стандартных UNIX-паролей [8].

Однако эта схема наиболее уязвимо с точки зрения безопасности - пароль может быть перехвачен и использован другим лицом. Многие инциденты в сети Internet произошли отчасти из-за уязвимости традиционных паролей. Злоумышленники могут наблюдать за каналами в сети Internet и перехватывать передающиеся в них открытым текстом пароли, поэтому схему аутентификации с традиционными паролями следует признать устаревшей.

Для преодоления этого недостатка разработан ряд средств усиленной аутентификации: смарт-карты, персональные жетоны, биометрические механизмы и т.п. Хотя в них задействованы разные механизмы аутентификации, общим для них является то, что пароли, генерируемые этими устройствами, не могут быть повторно использованы нарушителем, наблюдающим за установлением связи. Поскольку проблема с паролями в сети Internet является постоянной, межсетевой экран для соединения с Internet, не располагающий средствами усиленной аутентификации или не использующий их, теряет всякий смысл.

Ряд наиболее популярных средств усиленной аутентификации, применяемых в настоящее время, называются системами с одноразовыми паролями. Например, смарт-карты или жетоны аутентификации генерируют информацию, которую хост-компьютер использует вместо традиционного пароля. Результатом является одноразовый пароль, который, даже если он будет перехвачен, не может быть использован злоумышленником под видом пользователя для установления сеанса с хост - компьютером.

Так как межсетевые экраны могут централизовать управление доступом в сети, они являются подходящим местом для установки программ или устройств усиленной аутентификации. Хотя средства усиленной аутентификации могут

использоваться на каждом хост - компьютере, более практично их размещение на межсетевом экране [6].

Если хост - компьютеры не применяют мер усиленной аутентификации, злоумышленник может попытаться взломать пароли или перехватить сетевой трафик с целью найти в нем сеансы, в ходе которых передаются пароли.

В этом случае сеансы TELNET или FTP, устанавливаемые со стороны сети Internet с системами сети, должны проходить проверку с помощью средств усиленной аутентификации, прежде чем они будут разрешены, Системы сети могут запрашивать для разрешения доступа и статические пароли, но эти пароли, даже если они будут перехвачены злоумышленником, нельзя будет использовать, так как средства усиленной аутентификации и другие компоненты межсетевого экрана предотвращают проникновение злоумышленника или обход ими межсетевого экрана.

При подключении корпоративной или локальной сети к глобальным сетям администратор сетевой безопасности должен решать следующие задачи:

– защита корпоративной или локальной сети от несанкционированного доступа со стороны глобальной сети;

– скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети,

– разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть.

Необходимость работы с удаленными пользователями требует установки жестких ограничений доступа к информационным ресурсам защищаемой сети. При этом часто возникает потребность в организации в составе корпорационной сети нескольких сегментов с разными уровнями защищенности:

– свободно доступные сегменты (например, рекламный WWW-сервер),

– сегмент с ограниченным доступом (например, для доступа сотрудникам организации с удаленных узлов),

– закрытые сегменты (например, локальная финансовая сеть организации).

Для защиты корпоративной или локальной сети применяются следующие основные схемы организации межсетевых экранов:

– межсетевой экран - фильтрующий маршрутизатор;

– межсетевой экран на основе двупортового шлюза;

– межсетевой экран на основе экранированного шлюза;

– межсетевой экран – экранированная подсеть.

2.4. Структура и возможности межсетевых экранов

Межсетевой экран, основанный на фильтрации пакетов, является самым распространенным и наиболее простым в реализации. Он состоит из фильтрующего маршрутизатора, расположенного между защищаемой сетью и сетью Internet. Фильтрующий маршрутизатор сконфигурирован для блокирования или фильтрации входящих и исходящих пакетов на основе анализа их адресов и портов. Компьютеры, находящиеся в защищаемой сети, имеют прямой доступ в сеть Internet, в то время как большая часть доступа к ним из Internet блокируется. Часто блокируются такие опасные службы, как X Windows, NIS и NFS.

На рисунке 1 представлены возможности брандмауэра Windows.

Рисунок 1 – Возможности брандмауэра Windows

На рисунке 2 представлены ограничения брандмауэра Windows.

Рисунок 2 – Ограничения брандмауэра Windows

Межсетевой экран на базе двупортового прикладного шлюза включает двудомный хост-компьютер с двумя сетевыми интерфейсами. При передаче информации между этими интерфейсами и осуществляется основная фильтрация. Для обеспечения дополнительной защиты между прикладным шлюзом и сетью Internet обычно размещают фильтрующий маршрутизатор. В результате между прикладным шлюзом и маршрутизатором образуется внутренняя экранированная подсеть. Эту подсеть можно использовать для размещения доступных извне информационных серверов.

Межсетевой экран на основе экранированного шлюза объединяет фильтрующий маршрутизатор и прикладной шлюз, разрешаемый со стороны внутренней сети. Прикладной шлюз реализуется на хост – компьютере и имеет только один сетевой интерфейс [10].

Межсетевой экран, состоящий из экранированной подсети, представляет собой развитие схемы межсетевого экрана на основе экранированного шлюза. Для создания экранированной подсети используются два экранирующих маршрутизатора. Внешний маршрутизатор располагается между сетью Internet и экранируемой подсетью, а внутренний - между экранируемой подсетью и защищаемой внутренней сетью.

Таким образом, в данной главе было рассмотрено использование и настройка брандмауэра.

ЗАКЛЮЧЕНИЕ

Мало кто сегодня не слышал об угрозах, существующих в виртуальном пространстве. Пока еще остается непреложным тот факт, что компьютер, подсоединенный к сети Интернет, может подвергнуться реальным атакам. Чтобы защититься от них, прежде всего нужен хороший брандмауэр.

Брандмауэр (межсетевой экран) – это система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения информации из одной части в другую. Брандмауэры представляют собой целый класс систем, порой сопоставимых по сложности с операционной системой.

Сетевой экран функционирует как пограничный блокпост, который пропускает трафик и в соответствии со списком правил не дает проникнуть в систему запрещенной информации.

Брандмауэры можно классифицировать по следующим критериям:

– по исполнению: программные, аппаратные и смешанного типа (аппаратно-программного);

– по компонентной модели: локальные (работающие на одном хосте) и распределенные (distributed firewall);

– по уровню, на котором функционируют брандмауэры: пакетный, прикладной, уровень соединения.

Функциональные требования к межсетевым экранам включают:

– требования к фильтрации на сетевом уровне;

– требования к фильтрации на прикладном уровне;

– требования по настройке правил фильтрации и администрированию;

– требования к средствам сетевой аутентификации;

– требования по внедрению журналов и учету.

Большинство компонентов межсетевых экранов можно отнести к одной из трех категорий:

– фильтрующие маршрутизаторы;

– шлюзы сетевого уровня;

– шлюзы прикладного уровня.

Шлюз сетевого уровня иногда называют системой трансляции сетевых адресов или шлюзом сеансового уровня модели OSI. Такой шлюз исключает, прямое взаимодействие между авторизированным клиентом и внешним хост-компьютером. Шлюз сетевого уровня принимает запрос доверенного клиента на конкретные услуги, и после проверки допустимости запрошенного сеанса устанавливает соединение с внешним хост – компьютером.

Одним из важных компонентов концепции межсетевых экранов является аутентификация (проверка подлинности пользователя). Прежде чем пользователю будет предоставлено право воспользоваться тем или иным сервисом, необходимо убедиться, что он действительно тот, за кого себя выдает. Одним из способов аутентификации является использование стандартных UNIX-паролей.

Межсетевой экран, основанный на фильтрации пакетов, является самым распространенным и наиболее простым в реализации. Он состоит из фильтрующего маршрутизатора, расположенного между защищаемой сетью и сетью Internet.

Межсетевой экран, состоящий из экранированной подсети, представляет собой развитие схемы межсетевого экрана на основе экранированного шлюза. Для создания экранированной подсети используются два экранирующих маршрутизатора. Внешний маршрутизатор располагается между сетью Internet и экранируемой подсетью, а внутренний - между экранируемой подсетью и защищаемой внутренней сетью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Артамонова, Н.В. Операционные системы для организации производства в промышленности: Учебное пособие / Н.В. Артамонова. – СПб.: ГУАП, 2016. – 224 с.
2. Астахова, И.Ф. Компьютерные науки. Деревья, операционные системы, сети / И.Ф. Астахова, И.К. Астанин и др. – М.: Физматлит, 2013. – 88 с.
3. Баула, В. Г. Архитектура ЭВМ и операционные среды : учебник / В. Г. Баула, А. Н. Томилин, Д. Ю. Волканов. – 2-е изд., стер. – М. : Академия, 2012. – 336 с.
4. Дейтел, Х., М. Операционные системы. Основы и принципы. Т. 1 / Х. М. Дейтел, Д.Р. Чофнес. - М.: Бином, 2016. – 1024 с.
5. Дейтел, Х.М. Операционные системы. Т. 2. Распределенные системы, сети, безопасность / Х.М. Дейтел, П.Д. Дейтел, Д.Р. Чофнес; Пер. с англ. С.М. Молявко. – М.: БИНОМ, 2013. – 704 с.
6. Иртегов, Д.В. Введение в операционные системы / Д. Иртегов. – СПб.: BHV, 2015. – 1040 с.
7. Карасева, М.В. Операционные системы. Практикум для бакалавров / М.В. Карасева. – М.: КноРус, 2016. – 376 с.
8. Коньков, К.А. Устройство и функционирование ОС Windows. Практикум к курсу "Операционные системы": Учебное пособие / К.А. Коньков. – М.: Бином, 2016. – 207 с.
9. Мартемьянов, Ю.Ф. Операционные системы. Концепции построенияи обеспечения безопасности / Ю.Ф. Мартемьянов и др. – М.: ГЛТ, 2016. – 332 с.
10. Назаров, С.В. Операционные системы. Практикум: Учебное пособие / С.В. Назаров, Л.П. Гудыно, А.А. Кириченко. – М.: КноРус, 2016. – 376 с.
11. Общее описание брандмауэров [Электронный ресурс]. – Режим доступа: https://compress.ru/article. aspx?id=9917
12. Партыка, Т. Л. Вычислительная техника : учеб. пособие / Т. Л. Партыка, И. И. Попов. – М. : ФОРУМ: ИНФРА-М, 2007. – 608 с.

13. Синицын, С.В. Операционные системы: Учебник для студентов учреждений высш. проф. образования / С.В. Синицын, А.В. Батаев, Н.Ю. Налютин. – М.: ИЦ Академия, 2016. – 304 с.
14. Стащук, П.В. Краткое введение в операционные системы: Учебное пособие / П.В. Стащук. – М.: Флинта, МПСУ, 2016. – 128 с.
15. Тюрин, И.В. Вычислительная техника и информационные технологии : учеб. пособие / И. В. Тюрин. – Ростов н/Д : Феникс, 2017. – 462 с.
16. Что такое брандмауэр, зачем он нужен, как его включить и настроить – пошаговое руководство [Электронный ресурс]. – Режим доступа: https://pronashkomp.ru/chto-takoye-brandmauer