Содержание:

Введение

По мере развития рыночных отношений обеспечение безопасности информации с каждым годом становится всё более актуально.
Большинство современных корпоративных информационных систем используют сети общего пользования, чтобы получить доступ к внешним ресурсам, предоставить собственные ресурсы внешним пользователям, а зачастую используют публичные сети как средство организации информационного взаимодействия территориально-распределенных участков корпоративных сетей. Так с одной стороны возникает необходимость обеспечения доступности части корпоративных информационных ресурсов извне, а также ресурсов внешних открытых сетей для внутренних пользователей компании, с другой – остро встает проблема контроля информационного взаимодействия с внешним миром и обеспечения защиты корпоративной информационной системы от угроз информационной безопасности извне.
Чтобы разграничить доступ к ресурсам и контролировать информационные потоки между защищаемой сетью компании и внешними сетями, а также между отдельными частями корпоративной сети, необходимо использовать специальные средства защиты – межсетевые экраны.

СУЩНОСТЬ И ПОНЯТИЕ МЕЖСЕТЕВЫХ ЭКРАНОВ

Определение сущности МЭ
По материалам руководящего документа Государственной технической комиссии

России межсетевой экран (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, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.
Такие понятия как межсетевой экран, firewall, брандмауэр, шлюз с установленным дополнительным программным обеспечением firewall, можно использовать как эквивалентные.
Основная задача межсетевого экрана состоит в проверке всех данных, которые поступают на компьютер и с него отправляются. Это средство работает как барьерный фильтр, отделяющий поступающие с компьютера данные от интернета. МЭ проверяет данные, после чего разрешает или блокирует их отправку в зависимости от типа, отправителя и получателя данных или их области применения.
То есть формальная постановка задачи экранирования, такова. Пусть существует два множества информационных систем. Экран – это средство разграничения доступа клиентов из одного множества к серверам другого множества. Экран реализует свои функции, контролируя все информационные потоки между двумя множествами систем. Контроль потоков заключается в их фильтрации, возможно, с выполнением некоторых преобразований.

Экран как средство разграничения доступа.
На следующем уровне детализации экран (полупроницаемую мембрану) удобнее представить как последовательность фильтров, каждый из которых, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за экран. Также допускаются преобразования данных, передача части данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю.

Экран как последовательность фильтров
Кроме функций разграничения доступа, экраны выполняют протоколирование обмена информацией.
МЭ находится между защищаемыми (внутренними) сетями и внешней средой (внешними сетями или другими сегментами корпоративных сетей). В первом случае говорят о внешнем межсетевом экране, во втором – о внутреннем.
МЭ является идеальным местом для встраивания средств активного аудита. Он может реализовать сколь угодно мощную реакцию на подозрительную активность,

вплоть до разрыва связи с внешней средой.
На межсетевой экран целесообразно возложить идентификацию/ аутентификацию внешних пользователей, которые нуждаются в доступе к корпоративным ресурсам.
В силу принципов эшелонированности обороны для защиты внешних подключений, как правило, используется двухкомпонентное экранирование. Первичная фильтрация реализуется граничным маршрутизатором, за которым располагается демилитаризованная зона (сеть с умеренным доверием безопасности, куда выносятся внешние информационные сервисы организации – электронная почта, Web и т.д.) и основной брандмауэр, который защищает внутреннюю часть корпоративных сетей.

Двухкомпонентное экранирование с демилитаризованной зоной.
В теории МЭ (особенно внутренний) должен быть многопротокольным, но на практике доминирование семейства протоколов TCP/IP настолько велико, что поддержка других протоколов кажется излишней и вредной для безопасности.
И внешний и внутренний МЭ может стать узким местом, так как объем сетевого трафика имеет тенденцию к быстрому росту. Одним из решений данной проблемы является разбиение межсетевого экрана на несколько аппаратных частей и организация специализированных серверов-посредников. Основной МЭ проводит грубую классификацию входящего трафика по видам и передоверяет фильтрацию соответствующим посредникам (например, посреднику, анализирующему HTTP-трафик). Сначала исходящий трафик обрабатывается сервером-посредником, который выполняет и функционально полезные действия, такие как кэширование страниц внешних Web-серверов, что снижает нагрузку на основной межсетевой экран в частности и сеть вообще.
Ситуации, в которых корпоративная сеть содержит лишь один внешний канал, скорее исключение, чем правило. Большинство корпоративных сетей состоит из нескольких территориально разнесенных сегментов, подключенных к Internet. Тогда каждое подключение должно быть защищено отдельным экраном. Можно считать, что корпоративный внешний МЭ является составным (распределенным), и требуется решать задачу согласованного администрирования всех компонентов.
Также существуют персональные межсетевые экраны. Они предназначены для защиты отдельных компьютеров. Главным отличием персональных межсетевых экранов от распределенных является наличие функции централизованного управления. Если персональными МЭ можно управлять только с того компьютера, на котором они установлены, и те идеально подходят для домашнего применения, то распределенными МЭ можно управлять централизованно, с единой консоли

управления. Такие отличия позволяют некоторым производителям выпускать свои решения в двух версиях - персональной (для домашних пользователей) и распределенной (для корпоративных пользователей).

КЛАССИФИКАЦИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ

Фильтрующие маршрутизаторы

Фильтрующий маршрутизатор представляет собой работающую на сервере программу, сконфигурированную таким способом, чтобы фильтровать входящие и исходящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов.

Решение о том, пропускать данный пакет или нет, принимается на основе следующей информации:

• IP-адреса отправителей и получателей;
• номера портов отправителей и получателей;
• флаги.

По сути дела, задача администратора заключается в составлении простой таблицы, на основании которой осуществляется фильтрация.

Некоторые маршрутизаторы сначала проверяют, с какого сетевого интерфейса маршрутизатора пришел пакет, а потом используют эту информацию как дополнительный критерий фильтрации.

Фильтрацию можно реализовать различными способами для блокирования соединений с определенными компьютерами или портами. Например, могут быть блокированы соединения, идущие от адресов тех компьютеров и сетей, которые считаются ненадежными или враждебными.

Правила фильтрации пакетов формулируются сложно, к тому же, из средств для проверки их корректности обычно существует только медленное ручное тестирование. Вместе с тем в отсутствие фильтрующего маршрутизатора средств протоколирования такие пакеты не смогут быть выявлены до обнаружения последствий проникновения. Даже если администратору сети удастся создать эффективные правила фильтрации, их возможности останутся ограниченными.

Например, маршрутизатору будет задано правило, в соответствии с которым он должен отбраковывать все пакеты с неизвестным адресом отправителя. Однако в данном случае хакер для проникновения внутрь защищенной сети может осуществить атаку, которую называют подменой адреса. При таких условиях фильтрующий маршрутизатор не сумеет отличить поддельный пакет от настоящего и пропустит его.

Положительные качества фильтрующих маршрутизаторов:

• относительно невысокая стоимость;
• гибкость в определении правил фильтрации;
• небольшая задержка при прохождении пакетов.

Недостатки фильтрующих маршрутизаторов:

• внутренняя сеть видна (маршрутизируется) из сети Интернет;
• правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;
• при нарушении работоспособности МЭ с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;
• отсутствует аутентификация на пользовательском уровне.

2.2 Шлюзы уровня приложений

Фильтрация на уровне пакетов пусть и проста, но порой явно недостаточна. Информации сетевого и транспортного уровня модели OSI иногда не хватает для эффективной работы, что обосновывает существование систем, работающих на самом верхнем уровне – прикладном. Для защиты ряда уязвимых мест, которые присущи фильтрующим маршрутизаторам, межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, как HTTP, FTP, Telnet и др. Подобные приложения называются proxy-службами, а хост, на котором работают proxy-службы, — шлюзом уровня приложений. Такой шлюз исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне.

Как только шлюз приложений обнаруживает сетевой сеанс, он останавливает его и вызывает уполномоченное приложение для оказания завершаемой услуги. Иногда шлюзы уровня приложений и фильтрующие маршрутизаторы объединяют в одном межсетевом экране для достижения более высокого уровня гибкости и безопасности.

Шлюзы прикладного уровня обеспечивают более высокую защиту, так как взаимодействие с внешним миром реализуется через небольшое число уполномоченных приложений, которые полностью контролируют весь входящий и

исходящий трафик. Следует отметить, что шлюзы уровня приложений требуют отдельного приложения для каждого сетевого сервиса.
К преимуществам шлюзов прикладного уровня можно отнести:
• невидимость структуры защищаемой сети из глобальной сети Интернет. Имена внутренних систем не обязательно сообщать внешним системам через DNS, т.к. шлюз прикладного уровня может быть единственным хостом, имя которого будет известно внешним системам;
• надежная регистрация и аутентификация. Прикладной трафик может быть аутентифицирован, прежде чем он достигнет внутренних хостов, и зарегистрирован более эффективно, чем с помощью стандартной регистрации;
• приемлемое соотношение цены и эффективности. Дополнительные программные или аппаратные средства аутентификации или регистрации нужно устанавливать только на шлюзе прикладного уровня;
• простые правила фильтрации. Правила на фильтрующем маршрутизаторе, не такие сложные, как на маршрутизаторе, который самостоятельно фильтрует прикладной трафик и отправляет его большому числу внутренних систем;
• возможность организации большого числа проверок. Защита на уровне приложений позволяет выполнять большое количество дополнительных проверок, что снижает вероятность взлома с использованием «дыр» в программном обеспечении.
Недостатки шлюзов уровня приложений следующие:
• сравнительно низкая производительность по сравнению с фильтрующими маршрутизаторами;
• более высокая стоимость по сравнению с фильтрующими маршрутизаторами.
Одним из важных элементов концепции межсетевых экранов является аутентификация (проверка подлинности пользователя), то есть пользователь получает право воспользоваться тем или иным сервисом только после того, как будет установлено, что он действительно тот, за кого себя выдает. При этом считается, что сервис для данного пользователя разрешен (процесс определения, какие сервисы разрешены конкретному пользователю, называется авторизацией). При получении запроса на использование сервиса от имени какого-либо пользователя межсетевой экран проверяет, какой способ аутентификации определен для данного субъекта, и передает управление серверу аутентификации. После получения положительного ответа от сервера аутентификации межсетевой экран осуществляет запрашиваемое пользователем соединение. Большое число коммерческих межсетевых экранов поддерживает несколько различных схем аутентификации и предоставляет администратору сетевой безопасности

возможность сделать выбор наиболее приемлемой в сложившихся условиях схемы.

Шлюзы сеансового уровня

Данный класс маршрутизаторов представлен как система, транслирующая соединение с внешними узлами. Шлюз принимает запрос авторизованного клиента на определенные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с местом назначения (внешним хостом). Затем шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации. Пункт назначения задается заранее, источников при этом может быть очень много. Используя различные порты, можно создавать разные конфигурации соединений. Такой тип шлюза позволяет создать транслятор TCP-соединения для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису и сбор статистики по его использованию.

Шлюз следит за квитированием (подтверждением) связи между авторизованным клиентом и внешним хостом, он определяет, является ли запрашиваемый сеанс связи допустимым. Когда авторизованный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли данный клиент базовым критериям фильтрации. Далее, действуя от имени клиента, шлюз устанавливает соединение с внешним хостом и следит за выполнением процедуры квитирования связи по протоколу TCP. Эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить).

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число, например 500, является запросом клиента на открытие сеанса. Внешний хост, получивший этот пакет, посылает в ответ другой, помеченный флагом ACK и содержащий число на единицу большее, чем в принятом пакете (в данном случае 501), подтверждая тем самым прием пакета SYN от клиента. Затем осуществляется обратная процедура: хост посылает клиенту пакет SYN с исходным числом, например 700, а клиент подтверждает его получение передачей пакета ACK, содержащего число 701. На этом процесс квитирования связи завершается.

Шлюз сеансового уровня признает завершенное соединение допустимым только в том случае, если при выполнении процедуры квитирования связи флаги SYN и ACK, а также числа, содержащиеся в TCP-пакетах, оказываются логически связанными между собой.

После того как шлюз определил, что доверенный клиент и внешний хост являются авторизованными участниками сеанса TCP, и проверил его допустимость, он устанавливает соединение. Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, не проводя никакой фильтрации. Он поддерживает таблицу установленных соединений, пропуская данные, которые

относятся к одному из сеансов связи, зафиксированных в данной таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает сеть, использовавшуюся в текущем сеансе.
Недостатком шлюзов сеансового уровня является отсутствие проверки содержимого передаваемых пакетов, что дает возможность нарушителю проникнуть через такой шлюз.

НЕДОСТАТКИ ПРИМЕНЕНИЯ МЕЖСЕТЕВЫХ ЭКРАНОВ

Недостатки использования межсетевых экранов
Межсетевые экраны используются при организации защищенных виртуальных частных сетей. Несколько локальных сетей, подключенных к глобальной, объединяются в одну защищенную виртуальную частную сеть. Передача данных между этими локальными сетями является невидимой для пользователей, а конфиденциальность и целостность передаваемой информации должны обеспечиваться при помощи средств шифрования, использования цифровых подписей и т.п. При передаче данных может шифроваться не только содержимое пакета, но и некоторые поля заголовка.
Межсетевой экран не в состоянии решить все проблемы безопасности корпоративной сети. Помимо описанных выше достоинств межсетевых экранов имеется ряд ограничений в их использовании, а также существуют угрозы безопасности, от которых межсетевые экраны не могут защитить. Отметим наиболее существенные ограничения в применении межсетевых экранов:
• большое количество остающихся уязвимых мест. Межсетевые экраны не защищают от черных входов (люков) в сети. Например, если можно осуществить неограниченный доступ по модему в сеть, защищенную межсетевым экраном, атакующие могут эффективно обойти межсетевой экран;
• неудовлетворительная защита от атак сотрудников компании. Межсетевые экраны обычно не обеспечивают защиты от внутренних угроз;
• ограничение в доступе к нужным сервисам. Самый очевидный недостаток межсетевого экрана заключается в том, что он может блокировать ряд сервисов,

которые применяют пользователи, — Telnet, FTP и др. Для решения подобных проблем требуется проведение хорошо продуманной политики безопасности, в которой будет соблюдаться баланс между требованиями безопасности и потребностями пользователей;
• концентрация средств обеспечения безопасности в одном месте. Это позволяет легко осуществлять администрирование работы межсетевого экрана;
• ограничение пропускной способности, так как все соединения должны осуществляться только через МЭ, а в некоторых случаях, кроме всего прочего, еще и подвергаться фильтрации.
Следует учитывать, что межсетевые экраны не защищают от загрузки пользователями зараженных вирусами программ из Интернета или от передачи таких программ по средством электронной почты. Но, несмотря на вышеперечисленные недостатки можно с уверенностью утверждать, что применение межсетевого экрана не будет лишним, это подтверждает существующая на сегодняшний день позиция, по отношению к данному средству защиты, в IT кругах.

ПРОГРАММНЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ

Сравнительные характеристики программных МЭ
К основным характеристикам персональных МЭ относят следующие:
1) фильтрация активного контента в веб-трафике – возможность блокировки элементов ActiveX, апплетов Java, скриптов JavaScript и VBScript, всплывающих окон в загружаемых пользователем веб-страницах;
2) фильтрация активного контента в почтовом трафике – возможность блокировки того же самого в почтовых сообщениях;
3) поддержка ICS – поддержка Microsoft Internet Connection Sharing;
4) режим невидимости компьютера в сети. В обычном режиме при попытке доступа к закрытому порту коммуникационные компоненты ОС отправляют ответ о том, что данный порт закрыт или что данный сервис недоступен. Это дает возможность определить, что данная машина активна. В режиме невидимости такие ответ не отправляются;
5) режим невидимости пользователя – возможность блокировки cookies и

ссылок на предыдущий узел (referers). Это в какой-то степени не позволяет различным он-лайновым службам отслеживать перемещения пользователя и его повторные заходы на веб-сайты;
6) удаление баннеров – возможность блокировки (удаления) баннеров из загружаемых веб-страниц;
7) блокировка доступа к запрещенным узлам – возможность блокировки доступа к определенным веб-сайтам (Parental Control);
8) аутентификация приложений – возможность цифровой подписи приложений, получивший те или иные права доступа в сеть. Потенциально это позволяет блокировать доступ троянским программам, маскирующимся под легитимные приложения;
9) поддержка плагинов – возможность подключения дополнительных модулей для расширения базовой функциональности;
10) автоматическое обновление – возможность проверки на наличие новой версии ПО, его загрузки и обновления;
11)протоколирование – возможность протоколирования работы программы и сетевых событий (вторжений, входящего (исходящего) трафика и т.д.);
12) обнаружение сканирования – возможность обнаружения сканирования портов защищаемой системы;
13) обнаружение атаки – возможность обнаружения атаки на защищаемую систему;
14) удаленное администрирование – возможность удаленного управления программой (например, через специальный клиент или веб-браузер);
15) защита конфигурации по паролю – возможность установки пароля для защиты конфигурации программы от изменений;
Основные характеристики рассмотренных ранее программных МЭ представлены ниже в таблице.

Таблица. Сравнительные характеристики программных межсетевых экранов.

Продукт	Zone Alarm Pro	Outpost Firewall Pro	Norton Internet Security	AtGuard	Tiny Personal Firewall	BlackICE PC Protection	Kaspersky Anti-Hacker
Встроенный антивирус	-	-	+	-	+	-	-

Фильтрация активного контента в веб-трафике	+	+	+	+	+	-	+
Фильтрация активного контента в почтовом трафике	-	+	+	-	+	-	+
Поддержка ICS	+	+	+	-	+	+	+
Режим невидимости компьютера в сети	+	+	+	-	+	+	+
Режим невидимости пользователя	+	+	+	+	-	-	+
Удаление баннеров	+	+	+	+	-	-	-
Блокировка доступа к запрещенным узлам	-	+	+	-	-	-	+
Аутентификация приложений	+	+	+	-	+	+	+
Поддержка плагинов	-	+	+	-	-	-	-
Автоматическое обновление	-	+	+	-	-	-	+
Протоколирование	+	+	+	+	+	+	+

Обнаружение сканирования	+	+	+	-	+	+	+
Обнаружение атаки	+	+	+	-	+	+	+
Удаленное администрирование	-	-	-	-	-	+	-
Защита конфигурации по паролю	+	+	+	+	-	-	+

Символом «+» в таблице обозначены те характеристики, которыми обладают соответствующие межсетевые экраны.

РЕАЛИЗАЦИИ МЕЖСЕТЕВЫХ ЭКРАНОВ

Реализации межсетевых экранов

На сегодняшний день большое число иностранных и отечественных компаний предлагают различные аппаратно-программные и программные реализации межсетевых экранов.

Компания NetScreen Technologies обладает большим спектром продуктов, начиная с устройств, предоставляющих доступ отдельных пользователей к корпоративным сетям предприятий по защищенным каналам, и заканчивая моделями, которые предназначены для внедрения в структуры больших предприятий и создания систем безопасности с высокой пропускной способностью. Любой отдельный продукт из серии NetScreen является объединением межсетевого экрана и устройства VPN (virtual private network).

NetScreen-5 предлагает серию продуктов, которая позволяет создать межсетевые экраны с пропускной способностью 70 Мбит/с для модели NetScreen-5XT и 20 Мбит/с

для модели NetScreen-5XP, а также VPN с пропускной способностью 20 и 13 Мбит/с соответственно. Модель NetScreen-5XT может обеспечить 5 интерфейсов Fast Ethernet, в отличие от NetScreen-5XP, которая поддерживает до 5 портов 10Base-T. Оба эти продукта могут поддержать до 2 тысяч туннелей VPN и до 2 тысяч одновременных соединений TCP. Они комплектуются ОС NetScreen ScreenOS 4.0, которая используется для настройки физических и виртуальных интерфейсов в соответствии с требованиями безопасности.

Серия NetScreen-5 идеально подходит для установки между домашним компьютером пользователя и Web или для обеспечения защищенного доступа к локальным сетям предприятий.

Компания NetScreen Technologies разработала продукты серий NetScreen-25, -50, -100, -200 для внедрений на малых и средних предприятиях. Эти продукты способны создавать межсетевые экраны с пропускной способностью от 100 до 550 Мбит/с. К тому же по протоколу Triple DES со 168-битным ключом информация при шифровании передается между узлами по туннелю виртуальной частной сети на скорости от 20 до 200 Мбит/с. Продукты этих серий поддерживают от четырех до восьми портов Fast Ethernet.

Устройства NetScreen-500, NetScreen-1000 и NetScreen-5000 являются наилучшим решением для внедрения на крупных предприятиях, так какотличаются исключительной пропускной способностью. NetScreen-500 обеспечивает пропускную способность до 750 Мбит/с, а также VPN со скоростью 240 Мбит/с. NetScreen-5200 способна реализовать межсетевой экран с пропускной способностью 4 Гбит/с и VPN со скоростью до 2 Гбит/с. Она поддерживает до восьми портов Gigabit Ethernet или два порта Gigabit Ethernet и 24 Fast Ethernet. NetScreen-5400 обеспечивает скорость в 12 Гбит/с для межсетевого экрана и 6 Гбит/с для VPN. Она поддерживает до 78 портов Gigabit Ethernet и Fast Ethernet. Оба продукта способны поддерживать до 25 тыс. туннелей VPN и до миллиона одновременных соединений TCP. Они комплектуются ОС NetScreen ScreenOS 3.1. При этом каждый продукт компании NetScreen Technologies поддерживает протокол RADIUS (Remote Authentication Dial-In User Service — служба дистанционной аутентификации пользователей по коммутируемым линиям) и имеет собственную базу данных для аутентификации пользователей, подающих запрос на удаленный доступ.

Компания WatchGuard Technologies предлагает модели, которые можно использовать на мелких, средних и крупных предприятиях. Для мелких и средних предприятий были выпущены продукты серии Firebox III (4500, 2500, 1000, и 700). Модели Firebox 4500 и 2500 представлены как аппаратные МЭ под управлением

операционной системы Linux с защищенным ядром. Пропускная способность МЭ – 197 Мбит/с в режиме пакетной фильтрации и 60 Мбит/с — в режиме посредника (прозрачный proxy) на прикладном уровне. Брандмауэры имеют три сетевых интерфейса 10/100 Мбит/с Fast Ethernet. Оба МЭ могут поддерживать до 3 тыс. туннелей VPN, но модель FireBox 4500 позволяет достичь более высоких по сравнению с FireBox 2500 скоростей шифрования информации по алгоритму TripleDES — 100 и 55 Мбит/с соответственно.

Так же компания выпускает продукты Firebox SOHO 6, Firebox SOHO 6/tc и Firebox 700 для небольших и средних предприятий и для удаленных офисов.

Firebox 700 обслуживает одновременно около 250 пользователей. Это брандмауэр,поддерживающий как пакетную фильтрацию, так и фильтры — посредники приложений. В режиме пакетной фильтрации производительность Firebox 700 достигает 131 Мбит/с и 43 Мбит/с в режиме посредника. Firebox 700 способен создать виртуальную частную сеть с 150 туннелями одновременно и выполнять шифрование TripleDES со скоростью 5 Мбит/с.

Firebox SOHO 6 способен поддержать функционирование пакетных фильтров с пропускной способностью 75 Мбит/с. Так же он способен поддержать виртуальную частную сеть с пятью туннелями и пропускной способностью 20 Мбит/с (модификация SOHO/tc) и выполнять шифрование TripleDES.

Модель Firebox Vclass разработана для обеспечения высокоскоростной пропускной способности крупных информационных компаний и позволяет получить пропускную способность около 600 Мбит/с. Продукт поддерживает до 20 тыс. туннелей VPN и достигает скорости 300 Мбит/с в режиме шифрования.

Компания Cisco Systems предлагает серию межсетевых экранов Cisco PIX Firewall. Они обеспечивают высокий уровень производительности, надежности и безопасности. Модельный ряд брандмауэров представлен следующими продуктами: PIX 506E, 515E, 525 и 535.

Модели брандмауэров Cisco PIX 506E и 515E это модернизации Cisco PIX 506 и 515 соответственно. Они используются в корпоративных сетях небольших компаний и обеспечивают безопасность удаленных клиентов корпоративных сетей предприятий. Производительность модели 506E – 20 Мбит/с, а 515E — 188 Мбит/с. Шифрование потока данных может выполняться с использованием алгоритма DES с 56-битным ключом, а также TripleDES с 168-битным ключом. Cisco PIX 506E обладает пропускной способностью 20 Мбит/с при шифровании DES и 16 Мбит/с при TripleDES. Для модели 515E на алгоритме TripleDES скорость шифрования равна 63 Мбит/с. 515E поддерживает до 2 тыс. туннелей VPN.

Компания Cisco выпускает модели 525 и 535 для использования на предприятиях

среднего и крупного масштаба. Модель 525 имеет пропускную способность в 370 Мбит/с. Она может обслуживать до 280 тыс. сеансов одновременно. Производительность модели Cisco PIX 535 достигает 1 Гбит/с и VPN с пропускной способностью в 100Мбит/с. Также модель поддерживает до 500 тыс. одновременных соединений TCP и до 2 тыс. туннелей VPN.
В МЭ компании Cisco в качестве метода защиты используются разновидность алгоритма контекстной проверки Adaptive Security Algorithm (ASA) и внутренняя ОС PIX OS, позволяющие обеспечить высокую безопасность и надежность со стороны различных Интернет-атак.
В ноябре 2002 года компания eSoft, Inc. представила новую серию продуктов InstaGate xSP, которая пришла на смену ранним моделям InstaGate EX2 и InstaGate PRO. Под маркой InstaGate xSP компания eSoft выпускает InstaGate xSP Branch Office для небольших и распределенных офисов и InstaGate xSP Business для средних и больших офисов. Продукты серии xSP компания поставляет с пакетом приложений SoftPak, что позволяет пользователям легко и быстро создавать надежную систему безопасности всей корпоративной сети. Продукты xSP полностью совместимы с существующими моделями InstaGate, что позволяет создавать виртуальные частные сети на базе IPSec и PPTP. InstaGate xSP Branch Office поддерживает до 10 пользователей и 10 туннелей VPN, InstaGate xSP Business до 100 пользователей и 100 туннелей VPN. Эта серия отличается относительно небольшой стоимостью.
Компания 3Com предлагает на рынок два типа межсетевых экранов: OfficeConnect, предназначенные для небольших офисов, где число сотрудников менее ста, домашних офисов и работающих на дому специалистов, и SuperStack 3 – для штаб-квартир корпораций и крупных офисов, а также для клиентов, которым требуется высокопроизводительный доступ к виртуальной частной сети.
SuperStack 3 поддерживается неограниченное число пользователей корпоративной сети и обеспечивается до 1000 туннелей VPN. Пропускная способность данной модели составляет 45 Мбит/с, при шифровании алгоритмом TripleDES.
Модельный ряд OfficeConnect представлен моделями OfficeConnect Internet Firewall 25 и OfficeConnect InternetFirewall DMZ. OfficeConnect Internet Firewall DMZ использует порт DMZ, что позволяет обеспечить безопасный внешний доступ к ресурсам сети. OfficeConnect Internet Firewall DMZ поддерживает до 100 пользователей, а OfficeConnect Internet Firewall 25 — 25 пользователей. Совместно с брандмауэрами OfficeConnect Internet Firewall DMZ и OfficeConnect Internet Firewall 25 используется фильтр Web-сайтов OfficeConnect Web Site Filter, который обеспечивает фильтрацию доступа к нежелательным Web-сайтам. Все МЭ компании 3Com имеют сертификат ICSA. Компания 3Com выпускает межсетевые

экраны, в которых сочетается исключительная простота в использовании и гибкость выбора решений. МЭ компании 3Com легко устанавливаются и обеспечивают очень высокий уровень защиты. Установка в режиме plug-and-play исключает сложные и длительные процедуры настройки и администрирования без ущерба для строгости, полноты и детальности стратегии безопасности.
Так применение МЭ является ключевым элементом в построении безопасных, высокопроизводительных и надежных информационно-аналитических систем и систем автоматизации предприятий, распределенных баз данных, систем удаленного доступа работников к внутренним ресурсам корпоративных сетей, финансовых систем, сегментов корпоративной сети и корпоративной сети в целом.

Заключение

Основная проблема защиты информации сегодня – это построение комплексных систем защиты, отражающих, с одной стороны, типовые угрозы безопасности, а с другой – индивидуальную специфику конкретной информационной системы.
На сегодняшний день лучшей защитой от компьютерных преступников является межсетевой экран правильно установленный и подобранный для каждой сети. И хотя МЭ не гарантирует стопроцентную защиту от профессиональных взломщиков, но зато усложняет им доступ к сетевой информации, что касается любителей то для них доступ теперь считается закрытым. Также в будущем МЭ возможно станут лучшими защитниками для банков, предприятий, правительств, и других спецслужб. Также есть надежда, что когда-нибудь будет создан межсетевой экран, который никому не удастся обойти. На данном этапе программирования можно также заключить, что разработки по межсетевым экранам на сегодняшний день сулят в недалёком будущем весьма неплохие результаты.

Использованная литература

1. Абраменкова Ирина, Дьяконов Владимир, Пеньков Александр «Новые информационные технологии», Москва, 2006г.
2. Байбурин В.Б., Губенков А.А. Информационная безопасность. – М.: ЗАО «Новый издательский дом», 2005. – 128с.
3. Балдин Константин, Уткин Владимир «Информатика», Москва, 2003г.
4. Влад Максимов. Межсетевые экраны. Способы организации защиты.

http://www.lib.csu.ru/dl/bases/prg/kompress/articles/4311
5. Домашев А. В., Попов В. О., Правиков Д. И. и др. Программирование алгоритмов защиты информации. М.:Нолидж, 2000.
6. Дэвид В. Чепмен, мл., Энди Фокс Брандмауэры Cisco Secure PIX = Cisco® Secure PIX® Firewalls — М.: «Вильямс», 2003. — С. 384. — ISBN 1-58705-035-8.
7. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. М.: Телеком, 2000.
8. Мамаев М., Петренко С. Технологии защиты информации в интернете. СПб.: Питер, 2002.
9. Олгтри Т.В. Firewalls. Практическое применение межсетевых экранов.: ДМК Пресс, 2001. – 400с. – ISBN 5-94074-037-5
10. Фридланд А. «Основные ресурсы информатики», Москва, 2007г.