**Содержание:**


# Введение

С развитием рыночных отношений информация всё более и более приобретает качества товара, то есть её можно купить, продать, передать и, к сожалению, украсть. Поэтому проблема обеспечения безопасности информации с каждым годом становится всё более актуальной. Одним из возможных направлений решения данной проблемы является использование межсетевых экранов. В реферате на основе анализа российского рынка рассмотрены особенности и возможности использования наиболее эффективного в настоящее время и динамично развивающегося средства сетевой защиты — межсетевых экранов.

Современные технологии сетевой защиты являются одним из наиболее динамичных сегментов современного рынка обеспечения безопасности. Средства сетевой защиты настолько стремительно развиваются, что в настоящее время общепринятая терминология в данном направлении ещё окончательно не установилась. Эти средства защиты в литературе и средствах массовой информации фигурируют как firewall, брандмауэры и даже информационные мембраны. Но наиболее часто используется термин “межсетевые экраны” (МЭ).

В общем случае, для обеспечения сетевой защиты между двумя множествами информационных систем (ИС) ставится экран или информационная мембрана, которые являются средством разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве. В этом смысле МЭ можно представить как набор фильтров, анализирующих проходящую через них информацию и принимающих решение: пропустить информацию или её заблокировать. Одновременно с этим производится регистрация событий и тревожная сигнализация в случае обнаружения угрозы. Обычно экранирующие системы делаются несимметричными. Для экранов определяются понятия “внутри” и “снаружи”, причём, в задачу экрана входит защита внутренней сети от потенциально враждебного окружения. Кроме того, МЭ может использоваться в качестве корпоративной открытой части сети, видимой со стороны Internet. Так, например, во многих организациях МЭ используются для

хранения данных с открытым доступом, как, например, информации о продуктах и услугах, файлах из баз FTP, сообщений об ошибках и так далее.

Современные требования к межсетевым экранам

1. Основное требование — это обеспечение безопасности внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи.

2. Экранирующая система должна обладать мощными и гибкими средствами управления для простого и полного проведения в жизнь политики безопасности организации.

3. Межсетевой экран должен работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий.

4. Процессор межсетевого экрана должен быть быстродействующим, работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий поток в пиковых режимах, чтобы его нельзя было блокировать большим количеством вызовов и нарушить его работу.

5. Система обеспечения безопасности должна быть сама надежно защищена от любых несанкционированных воздействий, поскольку она является ключом к конфиденциальной информации в организации.

6. Система управления экранами должна иметь возможность централизованно обеспечивать проведение единой политики безопасности для удаленных филиалов.

7. Межсетевой экран должен иметь средства авторизации доступа пользователей через внешние подключения, что является необходимым в случаях работы сотрудников организации в командировках.

## Классификация межсетевых экранов

В настоящее время не существует единой и общепризнанной классификации межсетевых экранов. Выделим следующие классы межсетевых экранов:

- **Фильтрующие маршрутизаторы.**
- **Шлюзы сеансового уровня.**
- **Шлюзы уровня приложений.**

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

## Фильтрующие маршрутизаторы

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

Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы следующих полей заголовка пакета:

- IP-адрес отправителя;
- IP-адрес получателя;
- порт отправителя;
- порт получателя.

Некоторые маршрутизаторы проверяют, с какого сетевого интерфейса маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации.

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

Правила фильтрации пакетов формулируются сложно, к тому же обычно не существует средств для проверки их корректности, кроме медленного ручного тестирования. При этом в отсутствие фильтрующего маршрутизатора средств протоколирования (если правила фильтрации пакетов все-таки позволят опасным пакетам пройти через маршрутизатор) такие пакеты не смогут быть выявлены до обнаружения последствий проникновения. Даже если администратору сети удастся создать эффективные правила фильтрации, их возможности останутся ограниченными. Например, администратор задает правило, в соответствии с которым маршрутизатор будет отбраковывать все пакеты с неизвестным адресом

отправителя. Однако в данном случае хакер для проникновения внутрь защищенной сети может осуществить атаку, которую называют подменой адреса. В таких условиях фильтрующий маршрутизатор не сумеет отличить поддельный пакет от настоящего и пропустит его.

К положительным качествам фильтрующих маршрутизаторов можно отнести следующие:

- сравнительно 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 межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;
- отсутствует аутентификация на пользовательском уровне.

## Шлюзы сеансового уровня

Данный класс маршрутизаторов представляет собой транслятор TCP-соединения. Шлюз принимает запрос авторизованного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с местом назначения (внешним хостом). После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации. Как правило, пункт назначения задается заранее, в то время как источников может быть много. Используя различные порты, можно создавать разнообразные конфигурации соединений. Данный 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 подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым. Чтобы выявить допустимость запроса на сеанс связи, шлюз выполняет

следующую процедуру. Когда авторизованный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли данный клиент базовым критериям фильтрации. Затем, 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 нашем случае 501), подтверждая тем самым прием пакета SYN от клиента.

Далее 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.

## Шлюзы уровня приложений

С целью защиты ряда уязвимых мест, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, как Telnet и FTP. Подобное приложение называется proxy-службой, а хост, на котором работает proxy-служба, — шлюзом уровня приложений. Такой шлюз исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне.

Обнаружив сетевой сеанс, шлюз приложений останавливает его и вызывает уполномоченное приложение для оказания завершаемой услуги. Для достижения более высокого уровня безопасности и гибкости шлюзы уровня приложений и фильтрующие маршрутизаторы могут быть объединены в межсетевом экране.

Шлюзы прикладного уровня позволяют обеспечить надежную защиту, поскольку взаимодействие с внешним миром реализуется через небольшое число уполномоченных приложений, полностью контролирующих весь входящий и исходящий трафик. Следует отметить, что шлюзы уровня приложений требуют отдельного приложения для каждого сетевого сервиса.

По сравнению с работающими в обычном режиме, при котором прикладной трафик пропускается непосредственно к внутренним хостам, шлюзы прикладного уровня имеют ряд преимуществ:

- невидимость структуры защищаемой сети из глобальной сети Интернет. Имена внутренних систем можно не сообщать внешним системам через DNS, поскольку шлюз прикладного уровня может быть единственным хостом, имя которого будет известно внешним системам;
- надежная аутентификация и регистрация. 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 оказываются менее сложными, чем на маршрутизаторе, который самостоятельно фильтрует прикладной трафик и отправляет его большому числу внутренних систем. Маршрутизатор должен пропускать прикладной трафик, предназначенный только для шлюза прикладного уровня, и блокировать весь остальной;

- 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.

Недостатками шлюзов уровня приложений являются:

- относительно низкая производительность по сравнению с фильтрующими маршрутизаторами. В частности, при использовании клиент-серверных протоколов, таких как Telnet, требуется двухшаговая процедура для входных и выходных соединений;
- 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. Как правило, большинство коммерческих межсетевых экранов поддерживает несколько различных схем аутентификации, предоставляя администратору сетевой безопасности возможность сделать выбор наиболее приемлемой в сложившихся условиях схемы.

## Основные способы развертывания межсетевых экранов в корпоративных сетях

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

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

- скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;
- разграничение доступа в защищаемую сеть из глобальной и из защищаемой сети в глобальную.

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

- свободно доступные сегменты;
- сегменты с ограниченным доступом;
- закрытые сегменты.

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

1. **Межсетевой экран, представленный как фильтрующий маршрутизатор.**
2. **Межсетевой экран на основе двухпортового шлюза**.
3. **Межсетевой экран на основе экранированного шлюза.**
4. **Межсетевой экран с экранированной подсетью**.

## Межсетевой экран, представленный как фильтрующий маршрутизатор

Межсетевой экран, основанный на фильтрации пакетов, является самым распространенным и наиболее простым в реализации, представляя собой фильтрующий маршрутизатор, расположенный между защищаемой сетью и Интернетом.

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 Интернет, в то время как большая часть доступа к ним из Интернета блокируется. В принципе, фильтрующий маршрутизатор может реализовать любую из политик безопасности, описанных ранее. Однако если маршрутизатор не фильтрует пакеты по порту источника и номеру входного и выходного порта, то реализация политики

«запрещено все, что не разрешено» в явной форме может быть затруднена.

Межсетевые экраны, основанные на фильтрации пакетов, имеют те же недостатки, что и фильтрующие маршрутизаторы.

## Межсетевой экран на основе двухпортового шлюза

Межсетевой экран на базе двухпортового прикладного шлюза представляет собой хост с двумя сетевыми интерфейсами. При передаче информации между этими интерфейсами и осуществляется основная фильтрация. Для обеспечения дополнительной защиты между прикладным шлюзом и Интернетом размещают фильтрующий маршрутизатор. В результате между прикладным шлюзом и маршрутизатором образуется внутренняя экранированная подсеть. Ее можно использовать для размещения доступного извне информационного сервера. Размещение информационного сервера увеличивает безопасность сети, поскольку даже при проникновении на него злоумышленник не сможет получить доступ к системам сети через шлюз с двумя интерфейсами.

В отличие от схемы межсетевого экрана с фильтрующим маршрутизатором, прикладной шлюз полностью блокирует трафик IP между Интернетом и защищаемой сетью. Только уполномоченные приложения, расположенные на прикладном шлюзе, могут предоставлять услуги и доступ пользователям.

Данный вариант межсетевого экрана реализует политику безопасности, основанную на принципе «запрещено все, что не разрешено в явной форме»; при этом пользователю доступны только те службы, для которых определены соответствующие полномочия. Такой подход обеспечивает высокий уровень безопасности, поскольку маршруты к защищенной подсети известны лишь межсетевому экрану и скрыты от внешних систем.

Рассматриваемая схема организации межсетевого экрана относительно проста и достаточно эффективна. Поскольку межсетевой экран использует хост, то на нем могут быть установлены программы для усиленной аутентификации пользователей. Межсетевой экран может также протоколировать доступ, попытки зондирования и атак системы, что позволяет выявить действия злоумышленников.

# Межсетевой экран на основе экранированного шлюза

Межсетевой экран на основе экранированного шлюза обладает большей гибкостью по сравнению с межсетевым экраном, построенным на основе шлюза с двумя интерфейсами, однако эта гибкость достигается ценой некоторого уменьшения безопасности. Межсетевой экран состоит из фильтрующего маршрутизатора и прикладного шлюза, размещаемого со стороны внутренней сети. Прикладной шлюз реализуется на хосте и имеет только один сетевой интерфейс.

В данной схеме первичная безопасность обеспечивается фильтрующим маршрутизатором, который фильтрует или блокирует потенциально опасные протоколы, чтобы они не достигли прикладного шлюза и внутренних систем. Пакетная фильтрация в фильтрующем маршрутизаторе может быть реализована одним из следующих способов:

- внутренним хостам позволяется открывать соединения с хостами в сети Интернет для определенных сервисов (доступ к ним разрешается среде пакетной фильтрации);
- запрещаются все соединения от внутренних хостов (им надлежит использовать уполномоченные приложения на прикладном шлюзе).

В подобной конфигурации межсетевой экран может использовать комбинацию двух политик, соотношение между которыми зависит от конкретной политики безопасности, принятой во внутренней сети. В частности, пакетная фильтрация на фильтрующем маршрутизаторе может быть организована таким образом, чтобы прикладной шлюз, используя свои уполномоченные приложения, обеспечивал для систем защищаемой сети сервисы типа Telnet, FTP, SMTP.

Основной недостаток схемы межсетевого экрана с экранированным шлюзом заключается в том, что если атакующий нарушитель сумеет проникнуть в хост, перед ним окажутся незащищенными системы внутренней сети. Другой недостаток связан с возможной компрометацией маршрутизатора. Если маршрутизатор окажется скомпрометированным, внутренняя сеть станет доступна атакующему нарушителю.

# Межсетевой экран с экранированной подсетью

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 Интернетом и экранируемой подсетью, а внутренний — между экранируемой подсетью и защищаемой внутренней сетью. В экранируемую подсеть входит прикладной шлюз, а также могут включаться информационные серверы и другие системы, требующие контролируемого доступа. Эта схема межсетевого экрана обеспечивает высокий уровень безопасности благодаря организации экранированной подсети, которая еще лучше изолирует внутреннюю защищаемую сеть от Интернета.

Внешний маршрутизатор защищает от вторжений из Интернета как экранированную подсеть, так и внутреннюю сеть. Внешний маршрутизатор запрещает доступ из Глобальной сети к системам внутренней сети и блокирует весь трафик к Интернету, идущий от систем, которые не должны являться инициаторами соединений.

Этот маршрутизатор может быть использован также для блокирования других уязвимых протоколов, которые не должны передаваться к хост-компьютерам внутренней сети или от них.

Внутренний маршрутизатор защищает внутреннюю сеть от несанкционированного доступа как из Интернета, так и внутри экранированной подсети. Кроме того, он осуществляет большую часть пакетной фильтрации, а также управляет трафиком к системам внутренней сети и от них.

Межсетевой экран с экранированной подсетью хорошо подходит для защиты сетей с большими объемами трафика или с высокими скоростями обмена.

К его недостаткам можно отнести то, что пара фильтрующих маршрутизаторов нуждается в большом внимании для обеспечения необходимого уровня безопасности, поскольку из-за ошибок в их конфигурировании могут возникнуть провалы в системе безопасности всей сети. Кроме того, существует принципиальная возможность доступа в обход прикладного шлюза.

## Недостатки применения 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.

## Особенности современных межсетевых экранов

Таблица 1. Особенности межсетевых экранов

| Тип межсетевого экрана | Принцип работы | Достоинства |
| --- | --- | --- |
| Экранирующие маршрутизаторы (брандмауэры с фильтрацией пакетов) | Фильтрация пакетов осуществляется в соответствии с IP- заголовком пакета по критерию: то, что явно не запрещено, является разрешенным. Анализируемой информацией является:<br>адрес отправителя; адрес получателя;<br>информация о приложении или протоколе;<br>номер порта источника;<br>номер порта получателя. | Низкая стоимо<br>Минимальное в<br>производитель<br>Простота конф<br>установки<br>Прозрачность д<br>программного |
| Экранирующий шлюз (ЭШ) | Информационный обмен происходит через хост-бастион, установленный между внутренней и внешней сетями, который принимает решения о возможности маршрутизации трафика. ЭШ бывают двух типов: сеансового и прикладного уровня | Отсутствие скв<br>прохождения п<br>сбоев<br>Усиленные, по<br>ЭМ, механизмы<br>позволяющие и<br>дополнительны<br>аутентификаци<br>программные,<br>аппаратные<br>Использование<br>трансляции ад<br>позволяющей с<br>адресов хостов |

| | | |
|---|---|---|
| Экранирующие подсети (ЭП) | Создается изолированная подсеть, расположенная между внутренней и открытой сетями. Сообщения из открытой сети обрабатываются прикладным шлюзом и попадают в ЭП. После успешного прохождения контроля в ЭП они попадают в закрытую сеть. Запросы из закрытой сети обрабатываются через ЭП аналогично. Фильтрование осуществляется из принципа: то, что не разрешено, является запрещенным | Возможность с внутренней се Увеличение на защиты Возможность с большого траф внутренней и с сетями при исп нескольких хо в ЭП “прозрачность любых сетевых структуры вну |

## Сравнительные характеристики современных межсетевых экранов

Таблица 2. Сравнительные характеристики современных межсетевых экранов

| Продукт | Тип | Платформа | Компания | Особенности |
|---|---|---|---|---|
| Solstice Firewall - 1 | Комплексный экран | SunOS, UNIX, Solaris | Sun Microsystems | Реализует по безопасности имеющие явн отбрасывают работы филь шлюзах и сер записи обо вс запускают ме требующие р администрат |

| | | | | |
|---|---|---|---|---|
| Black Hole | Экранирующий шлюз прикладного уровня | Различные аппаратные платформы | Milkyway Networks Corporation | Не использу фильтрации Принцип дей не разрешен запрещенны все действия предупрежда нарушениях. Может испол двунаправле |
| BorderWare Firewall Server | Экранирующий шлюз прикладного уровня | UNIX, Windows, DOS | Secure Computing Corporation | Программное обеспечиваю под управлен (собственная Позволяет ф время, попыт протокол. |
| ALF (Application Layer Filter) | Экранирующий шлюз прикладного уровня | BSDI | SOS Corporation | Может фильт адресам, диа протоколам и Приходящий может пропу ликвидирова его адресу. |
| ANS InterLock Service | Экранирующий шлюз прикладного уровня | UNIX | ANS CO + RE Systems | Использует п посредники д HTTR. Поддер соединения т в качестве средств ауте могут исполь аппаратные. |

| | | | | |
|---|---|---|---|---|
| Brimstone | Комплексный экран | SunOS, BSDI на Intel, IRIX на INDY и Challenge | SOS Corporation | Для анализа дату, адрес, программы-п прикладного Telnet, FTR, S Gopher и др. большинство аутентифика |
| Centri | Экранирующий шлюз прикладного уровня | SunOS, BSDI, Solaris, HP- UX, AIX | Global Internet | Закрытая сет извне как еди Имеет прогр для служб: эл протокола FT все действия предупрежда |
| CONNECT | Экранирующий шлюз прикладного уровня | UNIX | Sterling Software | Является про продуктом, о защиту инфо НСД при соед открытой сет регистрирова сервера и пр возможных н |
| CyberGuard Firewall | Двунаправленный шлюз комплексного типа (хост-бастион как фильтр, шлюз прикладного уровня или комплексный экран) | Платформа RISC, OS UNIX | Harris Computer Systems Corporation | Использовани решения, вкл механизмы за и интегриров средства, пре RISC-компьют Для анализа исходный адр адрес назнач |

| | | | | |
|---|---|---|---|---|
| Digital Firewall for UNIX | Комплексный экран | Digital Alpha | Digital Equipment Corporation | Предустанав Digital Alpha возможности экранирующе прикладного |
| Eagle Enterprise | Экранирующий шлюз прикладного уровня | Реализация технологии Virtual Private Networking | Raptor Systems | Включает в с посредники для служб FT Регистрирует сервера и пр нарушениях. |
| Firewall IRX Router | Экранирующий маршрутизатор | DOS, MS-Windows | Livingston | Позволяет пр сети в целях опти трафика, безопасно св сеть с удален основе откры |
| Firewall-1 | Комплексный межсетевой экран | Intel x86, Sun Sparc и др. | Check Point Software Technologies | Обеспечивае хакерских на address-spoof адресов паке комбинацию сетевого и пр |

| | | | | |
|---|---|---|---|---|
| | | | | Представляе<br>интерфейс пр<br>API. Обеспечи |
| Firewall-1/<br>VPN-1 | Комплексный межсетевой экран | Intel x86, Sun Sparc и др. | Check Point Software Technologies | - выявление<br>вирусов;<br>- сканирован<br>- блокирован<br>- поддержку<br>- фильтраци<br>- обработку |
| TIS Firewall Toolkit | Набор программ для создания и управления системами firewall | BSD UNIX | Trusted Information Systems | Распространя<br>коде, все мод<br>языке C. Набо<br>программист |
| Gauntlet Internet Firewall | Экранирующий шлюз прикладного уровня | UNIX, Secured BSD | Trusted Information Systems | Поддерживае<br>электронная<br>терминальны<br>Возможности<br>сетевом уров<br>хакерских на<br>address-spoof<br>попыток изме<br>маршрутизац |
| FireWall/Plus | Мульти-протокольный межсетевой экран | Различные аппаратные платформы | Network-1 Software and Technology | Контроль реа<br>кадров, паке<br>приложений<br>протокола). П<br>более чем 39<br>возможность<br>условия филь<br>последующе |

| | | | | |
|---|---|---|---|---|
| Застава-Джет | Комплексный межсетевой экран | SPARC, Solaris, UNIX | Jet Infosystems | Реализует по безопасности имеющие явн отбрасывают российский с второму клас |

## Организация комплексной защиты корпоративной сети

Для защиты информационных ресурсов и обеспечения оптимальной работы распределенных корпоративных информационных систем необходимо применение комплексной системы информационной безопасности, которая позволит эффективно использовать достоинства межсетевых экранов и компенсировать их недостатки с помощью других средств безопасности.

Полнофункциональная защита корпоративной сети должна обеспечить:

- безопасное взаимодействие пользователей и информационных ресурсов, расположенных в экстранет- и интранет-сетях, с внешними сетями, например с Интернетом;
- технологически единый комплекс мер защиты для распределенных и сегментированных локальных сетей подразделений предприятия;
- наличие иерархической системы защиты, предоставляющей адекватные средства обеспечения безопасности для различных по степени закрытости сегментов корпоративной сети.

Характер современной обработки данных в корпоративных системах Интернет/интранет требует наличия у межсетевых экранов следующих основных качеств:

- мобильность и масштабируемость относительно различных аппаратно-программных платформ;
- возможность интеграции с аппаратно-программными средствами других производителей;
- простота установки, конфигурирования и эксплуатации;

- управление в соответствии с централизованной политикой безопасности.

В зависимости от масштабов организации и принятой на предприятии политики безопасности могут применяться различные межсетевые экраны. Для небольших предприятий, использующих до десятка узлов, подойдут межсетевые экраны с удобным графическим интерфейсом, допускающие локальное конфигурирование без применения централизованного управления. Для крупных предприятий предпочтительнее системы с консолями и менеджерами управления, которые обеспечивают оперативное управление локальными межсетевыми экранами, поддержку виртуальных частных сетей.

Увеличение потоков информации, передаваемых по Интернету компаниями и частными пользователями, а также потребность в организации удаленного доступа к корпоративным сетям являются причинами постоянного совершенствования технологий подключения корпоративных сетей к Интернету.

Следует отметить, что в настоящее время ни одна из технологий подключения, обладая высокими характеристиками по производительности, в стандартной конфигурации не может обеспечить полнофункциональной защиты корпоративной сети. Решение данной задачи становится возможным только при использовании технологии межсетевых экранов, организующей безопасное взаимодействие с внешней средой.

## Защита корпоративной сети от несанкционированного доступа из Интернет

При подключении сети предприятия к Интернету можно защитить корпоративную сеть от несанкционированного доступа с помощью одного из следующих решений:

- аппаратно-программный или программный межсетевой экран;
- маршрутизатор со встроенным пакетным фильтром;
- специализированный маршрутизатор, реализующий механизм защиты на основе списков доступа;
- операционная система семейства UNIX или, реже, MS Windows, усиленная специальными утилитами, реализующими пакетную фильтрацию.

Защита корпоративной сети на основе межсетевого экрана позволяет получить высокую степень безопасности и реализовать следующие возможности:

- семантическая фильтрация циркулирующих потоков данных;
- фильтрация на основе сетевых адресов отправителя и получателя;
- фильтрация запросов на транспортном уровне на установление виртуальных соединений;
- фильтрация запросов на прикладном уровне к прикладным сервисам;
- локальная сигнализация попыток нарушения правил фильтрации;
- запрет доступа неизвестного субъекта или субъекта, подлинность которого при аутентификации не подтвердилась;
- обеспечение безопасности от точки до точки: межсетевой экран, авторизация маршрута и маршрутизатора, туннель для маршрута и криптозащита данных и др.

Следует отметить, что межсетевые экраны позволяют организовать комплексную защиту корпоративной сети от несанкционированного доступа, основанную как на традиционной синтаксической (IP-пакетной) фильтрации контролируемых потоков данных, осуществляемой большинством ОС семейства Windows и UNIX, так и на семантической (контентной), доступной только коммерческим специальным решениям.

В настоящее время все выпускаемые межсетевые экраны можно классифицировать по следующим основным признакам:

1. по исполнению:

- аппаратно-программный,
- программный;

1. по функционированию на уровнях модели OSI:

- шлюз экспертного уровня,
- экранирующий шлюз (прикладной шлюз),
- экранирующий транспорт (шлюз сеансового уровня),
- экранирующий маршрутизатор (пакетный фильтр);

1. по используемой технологии:

- контроль состояния протокола,
- на основе модулей-посредников (proxy);

1. по схеме подключения:

- схема единой защиты сети,
- схема с защищаемым закрытым и не защищаемым открытым сегментами сети,
- схема с раздельной защитой закрытого и открытого сегментов сети.

Довольно распространенная на сегодня защита корпоративной сети на основе маршрутизатора со списком доступа основывается на использовании специализированных маршрутизаторов. Данная схема обладает высокой эффективностью и достаточной степенью безопасности. В качестве такого решения получили широкое распространение маршрутизаторы компании Cisco серий 12000, 7600. Для подключения сети предприятия к Интернету можно также использовать предшествующие серии маршрутизаторов этой фирмы.

Защита корпоративной сети на основе операционных систем, усиленных функциями пакетной фильтрации, построена на том, что системное программное обеспечение выполняет функции маршрутизации, фильтрации, сервисного обслуживания и др. По уровню надежности, безопасности и производительности наиболее предпочтительны решения на основе UNIX-подобной операционной системы.

## Организация внутренней политики безопасности корпоративной сети

В современных условиях более 50% различных атак и попыток доступа к информации осуществляется изнутри локальных сетей. Корпоративную сеть можно считать действительно защищенной от несанкционированного доступа только при наличии в ней как средств защиты точек входа со стороны Интернета, так и решений, обеспечивающих безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети предприятия. Безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети наилучшим образом обеспечивают решения на основе распределенных или персональных межсетевых экранов.

Внутренние корпоративные серверы компании, как правило, представляют собой приложения под управлением операционной системы Windows NT/2000, NetWare или, реже, семейства UNIX. По этой причине корпоративные серверы становятся потенциально уязвимыми к различного рода атакам.

Простейший способ защиты серверов — установка между серверами и Интернетом межсетевого экрана, например Firewall-1 компании Checkpoint. При правильной конфигурации большинство межсетевых экранов может защитить внутренние серверы от внешних злоумышленников, а некоторые выявляют и предотвращают атаки типа «отказ в обслуживании». Тем не менее этот подход не лишен некоторых недостатков. Когда корпоративные серверы защищены одним-единственным межсетевым экраном, все правила контроля доступа и данные оказываются сосредоточенными в одном месте. Таким образом, межсетевой экран становится узким местом и по мере нарастания нагрузки значительно теряет в производительности.

Альтернатива предыдущей схеме — приобретение дополнительных серверов и установка межсетевого экрана Firewall-1 компании Checkpoint или Cisco PIX компании Cisco перед каждым сервером. В результате того, что межсетевой экран становится выделенным ресурсом сервера, решается проблема узкого места и уменьшается влияние отказа отдельного межсетевого экрана на общее состояние сети. Однако и данный подход нельзя назвать идеальным, поскольку резко увеличиваются затраты компании на приобретение оборудования. К тому же возрастают трудозатраты на администрирование и обслуживание сети.

Наиболее удачным решением проблемы защиты корпоративных серверов представляется размещение средств безопасности на одной платформе с сервером, который они будут защищать. Эта задача выполняется путем использования распределенных или персональных межсетевых экранов, например CyberwallPLUS компании Network-1 Security Solution. Данные решения существенно дополняют функциональные возможности традиционных (периметровых) межсетевых экранов и могут использоваться для защиты как внутренних, так и Интернет-серверов.

В отличие от традиционных межсетевых экранов, представляющих собой, как правило, локальные «контрольные точки» контроля доступа к критическим информационным ресурсам корпорации, распределенные межсетевые экраны являются дополнительным программным обеспечением, которое надежно защищает корпоративные серверы, например Интернет-сервер.

Сравним традиционный и распределенный межсетевые экраны по нескольким показателям.

Эффективность. Традиционный межсетевой экран часто располагается по периметру, обеспечивая лишь один слой защиты. Персональный межсетевой экран функционирует на уровне ядра операционной системы и надежно защищает корпоративные серверы, проверяя все входящие и исходящие пакеты.

Простота установки. Традиционный межсетевой экран должен устанавливаться как часть конфигурации корпоративной сети. Распределенный межсетевой экран представляет собой программное обеспечение, которое устанавливается и удаляется в считанные минуты.

Управление. Традиционный межсетевой экран управляется сетевым администратором. Распределенный межсетевой экран может управляться либо сетевым администратором, либо пользователем локальной сети.

Производительность. Традиционный межсетевой экран является устройством обеспечения межсетевого обмена с фиксированным ограничением производительности по пакетам в секунду и не подходит для растущих серверных парков, соединенных друг с другом коммутированными местными сетями. Распределенный межсетевой экран позволяет наращивать серверные парки без ущерба принятой политике безопасности.

Стоимость. Традиционные межсетевые экраны, как правило, являются системами с фиксированными функциями и достаточно высокой стоимостью. Распределенные межсетевые экраны представляют собой программное обеспечение, стоимость которого, как правило, составляет от 20 до 10% от стоимости традиционных экранов. К примеру, распределенный межсетевой экран CyberwallPLUS компании Network-1 Security Solution стоит 6 тыс. долл., в то время как цена межсетевого экрана Cisco PIX 535 компании Cisco составляет порядка 50 тыс. долл.

Распределенные межсетевые экраны сочетают в себе средства контроля сетевого доступа со встроенными средствами выявления несанкционированного доступа и работают в режиме ядра, проверяя каждый пакет информации по мере его поступления из сети. Такие виды деятельности, как попытки взлома и несанкционированного доступа, блокируются этим экраном до перехода на уровень приложений сервера.

К основным преимуществам распределенных межсетевых экранов относятся:

- обеспечение безопасности входящего и исходящего трафика;

- обеспечение масштабируемой архитектуры путем распространения защиты с помощью межсетевого экрана на многочисленные серверы;
- устранение традиционного межсетевого экрана как единственного места сбоев;
- обеспечение недорогого, простого в реализации и управлении решения безопасности.

Таким образом, межсетевые экраны CyberwallPLUS обеспечивают дополнительный уровень защиты платформ под управлением операционной системы Windows NT/2000, на которых установлены корпоративные приложения, например Интернет-сервер. Кроме того, межсетевой экран CyberwallPLUS может предотвратить применение известных типов атак для вторжений на критичные серверы компании и сообщить администратору безопасности о подозрительной деятельности в сети.

Итак, межсетевой экран:

- защищает передаваемую информацию независимо от средств и среды передачи данных (спутниковые каналы, оптические линии связи, телефонные соединения, радиорелейные линии);
- выполняет защиту любых приложений, не требуя их изменений;
- прозрачен для конечных пользователей;
- позволяет реализовать масштабируемые системы защиты с возможностью дальнейшего их наращивания и усложнения по мере роста организаций и совершенствования требований политики безопасности;
- защищает отдельные сетевые информационные системы и приложения независимо от топологии сетей, которые они используют;
- защищает информационную систему предприятия от атак из внешней среды;
- защищает информацию от перехвата и изменения не только на внешних открытых соединениях, но и во внутренних сетях корпорации;
- может быть легко переконфигурирован по мере развития корпоративной политики информационной безопасности, добавления ресурсов, обновления технологий, роста сети корпорации.

## Реализации межсетевых экранов

В настоящее время большое количество как иностранных, так и отечественных компаний предлагают различные аппаратно-программные и программные реализации межсетевых экранов. Ниже приводится краткое описание некоторых

выпускаемых сегодня продуктов ведущих иностранных производителей.

Компания NetScreen Technologies предлагает широкий спектр продуктов, начиная от устройств, обеспечивающих доступ отдельных пользователей к корпоративной сети предприятия по защищенному каналу, и заканчивая моделями, предназначенными для внедрения в структуры больших предприятий и создания систем безопасности с высокой пропускной способностью. Каждый продукт серии NetScreen представляет собой комбинацию межсетевого экрана и устройства VPN (virtual private network).

Серия продуктов NetScreen-5 позволяет создавать межсетевой экран 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. В отличие от NetScreen-5XP, поддерживающей до пяти портов 10Base-T, модель NetScreen-5XT обеспечивает пять интерфейсов Fast Ethernet.

Оба продукта способны поддерживать до 2 тыс. туннелей VPN и до 2 тыс. одновременных соединений TCP. Они комплектуются операционной системой NetScreen ScreenOS 4.0, которая используется для настройки физических и виртуальных интерфейсов в соответствии с требованиями безопасности.

Продукты серии NetScreen-5 идеальным образом подходят для установки между домашним компьютером пользователя и Web или для обеспечения защищенного доступа к локальной сети предприятия.

Для внедрения на мелких и средних предприятиях компанией NetScreen Technologies разработаны продукты серий NetScreen-25, -50, -100, -200. Они позволяют создавать межсетевые экраны с пропускной способностью от 100 до 550 Мбит/с. К тому же данные при шифровании по протоколу Triple DES со 168-битным ключом передаются между узлами по туннелю виртуальной частной сети на скоростях от 20 до 200 Мбит/с. Эти серии продуктов поддерживают от четырех до восьми портов Fast Ethernet.

Семейство устройств NetScreen-500, NetScreen-1000 и NetScreen-5000 отличается исключительной пропускной способностью, поэтому является наилучшим решением для внедрения на крупных предприятиях. Модель NetScreen-500 обеспечивает пропускную способность почти 750 Мбит/с, а также VPN со скоростью 240 Мбит/с.

Модель NetScreen-5200 позволяет реализовать межсетевой экран с пропускной способностью 4 Гбит/с и VPN с 2 Гбит/с. Она поддерживает до восьми портов Gigabit Ethernet или два порта Gigabit Ethernet и 24 Fast Ethernet. Модель 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 операционной системой NetScreen ScreenOS 3.1. Кроме того, продукты компании NetScreen Technologies поддерживают протокол RADIUS (Remote Authentication Dial-In User Service — служба дистанционной аутентификации пользователей по коммутируемым линиям) и имеют собственную базу данных для аутентификации пользователей, подающих запрос на удаленный доступ.

Компания WatchGuard Technologies предлагает модели, предназначенные для внедрения как на мелких и средних, так и на крупных предприятиях. Для использования на предприятиях малого и среднего бизнеса предлагаются продукты серии Firebox III (4500, 2500, 1000, и 700). Модели Firebox 4500 и 2500 представляют собой аппаратные межсетевые экраны под управлением ОС Linux с защищенным ядром. Пропускная способность межсетевых экранов составляет 197 Мбит/с в режиме пакетной фильтрации и 60 Мбит/с — в режиме посредника (прозрачный proxy) на прикладном уровне. Каждый межсетевой экран имеет три сетевых интерфейса 10/100 Мбит/с Fast Ethernet.

Оба межсетевых экрана 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.

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

Firebox 700 способен обслуживать одновременно до 250 пользователей. Это межсетевой экран, поддерживающий как пакетную фильтрацию, так и фильтры — посредники приложений. Специалисты WatchGuard оценивают производительность Firebox 700 в 131 Мбит/с в режиме пакетной фильтрации и в 43 Мбит/с в режиме посредника. Firebox 700 позволяет создавать виртуальную частную сеть с 150 туннелями одновременно и выполнять шифрование TripleDES со скоростью 5 Мбит/с.

Firebox SOHO 6 поддерживает функционирование пакетных фильтров с пропускной способностью 75 Мбит/с. Он также поддерживает виртуальную частную сеть с пятью туннелями и пропускной способностью 20 Мбит/с (модификация SOHO/tc) при использовании шифрования TripleDES.

Для обеспечения высокоскоростной пропускной способности крупных информационных компаний разработана модель Firebox Vclass, позволяющая получить пропускную способность до 600 Мбит/с. Продукт способен поддерживать до 20 тыс. туннелей VPN. В режиме шифрования достигается скорость 300 Мбит/с.

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

Межсетевые экраны Cisco PIX 506E и 515E являются модернизациями моделей Cisco PIX 506 и 515 соответственно. Данные модели предназначены для использования в корпоративных сетях небольших компаний, а также для обеспечения безопасности удаленных клиентов корпоративных сетей предприятий. Модель 506E имеет производительность 20 Мбит/с, а 515E — 188 Мбит/с. Шифрование потока данных может осуществляться как с использованием алгоритма DES с 56-битным ключом, так и TripleDES с 168-битным ключом. Пропускная способность Cisco PIX 506E при шифровании DES — 20 Мбит/с, TripleDES — 16 Мбит/с. Скорость шифрования для модели 515E на алгоритме TripleDES равна 63 Мбит/с. Модель 515E поддерживает до 2 тыс. туннелей VPN.

Для использования на предприятиях среднего и крупного масштаба компания Cisco выпускает модели 525 и 535. Пропускная способность модели 525 составляет 370 Мбит/с. Данная модель может одновременно обслуживать до 280 тыс. сеансов. Модель Cisco PIX 535 имеет производительность 1 Гбит/с и поддерживает VPN с пропускной способностью 100 Мбит/с. Кроме того, эта модель поддерживает до 2 тыс. туннелей VPN и до 500 тыс. одновременных соединений TCP.

В качестве метода защиты в межсетевых экранах компании Cisco используются разновидность алгоритма контекстной проверки Adaptive Security Algorithm (ASA) и внутренняя операционная система PIX OS, позволяющие обеспечить высокую надежность и безопасность со стороны возможных Интернет-атак.

Компанией eSoft, Inc. в ноябре 2002 года представлена новая серия продуктов InstaGate xSP, которая пришла на смену более ранним моделям InstaGate EX2 и

InstaGate PRO. Под маркой InstaGate xSP компанией eSoft выпускаются InstaGate xSP Branch Office для небольших и распределенных офисов и InstaGate xSP Business для средних и больших офисов. Продукты серии xSP поставляются с пакетом приложений SoftPak, что позволяет пользователям быстро и легко создавать надежную систему безопасности всего периметра корпоративной сети. Серия продуктов xSP полностью совместима с существующими моделями InstaGate и позволяет создавать виртуальные частные сети на базе IPSec и PPTP. InstaGate xSP Branch Office поддерживает до 10 пользователей и 10 туннелей VPN, а InstaGate xSP Business до 100 пользователей и 100 туннелей VPN. Продукты этой серии отличаются относительно невысокой стоимостью.

Компания 3Com предлагает на рынок два типа межсетевых экранов: SuperStack 3, предназначенные для штаб-квартир корпораций и крупных офисов, а также для клиентов, которым требуется высокопроизводительный доступ к виртуальной частной сети, и OfficeConnect — для небольших офисов с числом сотрудников менее ста, домашних офисов и работающих на дому специалистов.

По оценкам производителей, SuperStack 3 поддерживает неограниченное число пользователей корпоративной сети и обеспечивает до 1000 туннелей VPN. Пропускная способность данной модели при шифровании алгоритмом TripleDES составляет 45 Мбит/с.

Модельный ряд OfficeConnect представлен моделями OfficeConnect Internet Firewall 25 и OfficeConnect Internet Firewall DMZ. Модель OfficeConnect Internet Firewall DMZ, используя порт DMZ, 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 межсетевыми экранами OfficeConnect Internet Firewall DMZ и OfficeConnect Internet Firewall 25 используется фильтр Web-сайтов OfficeConnect Web Site Filter, обеспечивающий фильтрацию доступа к нежелательным Web-сайтам. Все межсетевые экраны компании 3Com имеют сертификат ICSA. Семейство межсетевых экранов компании 3Com сочетает исключительную простоту в использовании с гибкостью выбора решений. Межсетевые экраны компании 3Com легко устанавливаются и обеспечивают чрезвычайно 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.

# Заключение

Таким образом, применение межсетевых экранов является ключевым элементом в построении высокопроизводительных, безопасных и надежных информационно-аналитических систем и систем автоматизации предприятий, финансовых систем, распределенных баз данных, систем удаленного доступа работников к внутренним ресурсам корпоративных сетей, сегментов корпоративной сети и корпоративной сети в целом.

**Литература**

Бюро научно-технической информации. http://www.bnti.ru/showart.asp?aid=449&lvl=03.07.05.

Влад Максимов. Межсетевые экраны. Способы организации защиты. http://www.lib.csu.ru/dl/bases/prg/kompress/articles/4311/