Московский гуманитарный университет экономики и права

Дипломная работа

Тема:

**«Анализ проблем информационной безопасности в компьютерной сети, организации подключенной к сети Интернтет»**

«Допущена к защите»

Декан финансово-учетного факультета

В.А. Дьеченко

Студент: Федин М.Ф.

Москва

2009

Содержание

Введение

1. Анализ проблем информационной безопасности в компьютерной сети организации подключенной к сети Интрентет. Современные подходы к их решению

1.1 Проблемы информационной безопасности современных компьютерных сетей организации

1.2 Вопросы информационных безопасности интернет – сервисов

1.3 Методы защиты компьютерной сети организации от НСД из сети Интернет. Применение межсетевых экранов

2. Теоретические вопросы построения межсетевых экранов

2.1 Архитектуры межсетевых экранов

2.2 Классификация межсетевых экранов

2.3 Различные типы окружений межсетевых экранов

2.4 Уровень защищенности межсетевых экранов

2.5 Виртуальные частные сети (VPN)

3. Предложение по совершенствованию защиты компьютерной сети организации за счет внедрение межсетевого экрана

3.1 Правильный выбор межсетевых экранов для защиты информации КСО

3.2 Intrusion Detection Systems (IDS)

3.3 IPv6 как сильное влияние на конструкцию межсетевого экрана

Заключения

Список сокращений и обозначений

Список использованных источников литературы

# Введение

Компьютеры, сети, Интернет стали неотъемлемой частью нашей повседневной жизни. Наш быстроразвивающийся, насыщенный технологиями мир с каждым днем все больше становится зависимым от компьютерных технологий и сетей. Однако эта зависимость возникла не внезапно. С каждым годом финансирование компьютерных технологий значительно возрастало, и неудивительно, что эти технологии проникли практически во все сферы деятельности человека.

На заре развития компьютерных технологий большинство людей не могли представить, насколько широко эти технологии будут использоваться в самом недалеком будущем. Поэтому, наверное, многие не решались уделять много времени и усилий для освоения того, что, в конце концов, могло оказаться обыкновенной забавой. По сравнению с требованиями современного рынка труда количество людей, работавших в то время в области компьютерных технологий, было ничтожно мало. Люди, работавшие в этом тесном сообществе, были хорошо знакомы и доверяли друг другу. Кроме того, в это сообщество допускались только избранные, которые заслуживали доверия. Таким образом, в те времена проблемы безопасности в области компьютерных технологий практически отсутствовали. И достаточно долгое время специалисты в области компьютерных технологий не уделяли внимания безопасности компьютерных сетей.

В настоящее время огромное количество сетей объединено посредством Интернет. Поэтому очевидно, что для безопасной работы такой огромной системы необходимо принимать определенные меры безопасности, поскольку практически с любого компьютера можно получить доступ к любой сети любой организации, причем опасность значительно возрастает по той причине, что для взлома компьютера к нему вовсе не требуется физического доступа.

Согласно данным, полученным Институтом компьютерной безопасности (Computer Security Institute) в результате недавно проведенного исследования, у 70% организаций были взломаны системы сетевой защиты, кроме того, 60% выявленных попыток взломов исходили из внутренних сетей организаций.

Учитывая эти факты, можно с уверенностью сказать, что проблема безопасности сетей остается неразрешенной и на сегодняшний день, поскольку у подавляющего большинства компаний не решены вопросы обеспечения безопасности, в результате чего они несут финансовые убытки.

Помимо кражи информации, опасность могут представлять атаки типа "отказ в обслуживании" и кража услуг.

Небольшие организации, до подключения к сети Интернет не сталкивавшиеся с вопросами защиты информации, часто оказываются полностью неподготовленными к изменившейся ситуации. Во многих случаях пользователи корпоративных сетей даже не подозревают о том, что их данные неожиданно оказались доступны любому пользователю Интернет

Одним из решений проблем безопасности подключения к сети Интернет является применение межсетевых экранов. Межсетевой экран - это программно-аппаратная система, находящаяся в точке соединения внутренней сети организации и Интернет и осуществляющая контроль передачи данных между сетями.

# 1. Анализ проблем информационной безопасности в компьютерной сети организации подключенной к сети Интрентет. Современные подходы к их решению

## Проблемы информационной безопасности современных компьютерных сетей организации

Новые информационные технологии активно внедряются во все сферы народного хозяйства. Появление локальных и глобальных сетей передачи данных предоставило пользователям компьютеров новые возможности оперативного обмена информацией. Если до недавнего времени подобные сети создавались только в специфических и узконаправленных целях (академические сети, сети военных ведомств и т.д.), то развитие Интернета и аналогичных систем привело к использованию глобальных сетей передачи данных в повседневной жизни практически каждого человека.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий.

Актуальность и важность проблемы обеспечения информационной

Безопасности обусловлены следующими факторами:

* Современные уровни и темпы развития средств информационной безопасности значительно отстают от уровней и темпов развития информационных технологий.
* Высокие темпы роста парка персональных компьютеров, применяемых в разнообразных сферах человеческой деятельности. Согласно данным исследований компании Gartner Dataquest в настоящее время в мире более миллиарда персональных компьютеров. А следующий миллиард будет достигнут уже в 2009 году.
* Резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;

Доступность средств вычислительной техники, и, прежде всего персональных ЭВМ, привела к распространению компьютерной грамотности в широких слоях населения. Это, в свою очередь, вызвало многочисленные попытки вмешательства в работу государственных и коммерческих систем, как со злым умыслом, так и из чисто «спортивного интереса». Многие из этих попыток имели успех и нанесли значительный урон владельцам информации и вычислительных систем. По неофициальным данным до 70% всех противо нарушений, совершаемых так называемыми хакерами, приходится на долю script-kiddies, в дословном переводе – дети, играющиеся со скриптами. Детьми их называют, потому что они не являются специалистами в компьютерных технологиях, но умеют пользоваться готовыми программными средствами, которые достают на хакерских сайтах в Интернете, для осуществления деструктивных действий.

* Значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средства автоматизации;

По оценкам специалистов в настоящее время около 70-90% интеллектуального капитала компании хранится в цифровом виде – текстовых файлах, таблицах, базах данных.

* Многочисленные уязвимости в программных и сетевых платформах;

Стремительное развитие информационных технологий открыло новые возможности для бизнеса, однако привело и к появлению новых угроз. Современные программные продукты из-за конкуренции попадают в продажу с ошибками и недоработками. Разработчики, включая в свои изделия всевозможные функции, не успевают выполнить качественную отладку создаваемых программных систем. Ошибки и недоработки, оставшиеся в этих системах, приводят к случайным и преднамеренным нарушениям информационной безопасности. Например, причинами большинства случайных потерь информации являются отказы в работе программно-аппаратных средств, а большинство атак на компьютерные системы основаны на найденных ошибках и недоработках в программном обеспечении. Так, например, за первые полгода после выпуска серверной операционной системы компании Microsoft Windows Server 2003 было обнаружено 14 уязвимостей, 6 из которых являются критически важными. Несмотря на то, что со временем Microsoft разрабатывает пакеты обновления, устраняющие обнаруженные недоработки, пользователи уже успевают пострадать от нарушений информационной безопасности, случившихся по причине оставшихся ошибок. Такая же ситуация имеет место и с программными продуктами других фирм. Пока не будут решены эти многие другие проблемы, недостаточный уровень информационной безопасности будет серьезным тормозом в развитии информационных технологий.

* Бурное развитие глобальной сети Интернет, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.

Подобная глобализация позволяет злоумышленникам практически из любой точки земного шара, где есть Интернет, за тысячи километров, осуществлять нападение на корпоративную сеть.

* Современные методы накопления, обработки и передачи информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям.

Например, в настоящее время в банковской сфере свыше 90% всех преступлений связано с использованием автоматизированных систем обработки информации.

Под угрозой безопасности понимается возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику или пользователю, проявляющегося в опасности искажения, раскрытия или потери информации.

Реализация той или иной угрозы безопасности может преследовать следующие цели:

* нарушение конфиденциальности информации. Информация, хранимая и обрабатываемая в компьютерной сети организации (КСО), может иметь большую ценность для ее владельца. Ее использование другими лицами наносит значительный ущерб интересам владельца;
* нарушение целостности информации. Потеря целостности информации (полная или частичная, компрометация, дезинформация) - угроза близкая к ее раскрытию. Ценная информация может быть утрачена или обесценена путем ее несанкционированного удаления или модификации. Ущерб от таких действий может быть много больше, чем при нарушении конфиденциальности;
* нарушение (частичное или полное) работоспособности КСО (нарушение доступности). Вывод из строя или некорректное изменение режимов работы компонентов КСО, их модификация или подмена могут привести к получению неверных результатов, отказу КСО от потока информации или отказам при обслуживании. Отказ от потока информации означает непризнание одной из взаимодействующих сторон факта передачи или приема сообщений. Имея в виду, что такие сообщения могут содержать важные донесения, заказы, финансовые согласования и т.п., ущерб в этом случае может быть весьма значительным.

Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Корпоративная информационная система (сеть) - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы (из закона об Электронно-цифровой подписи).

Компьютерные сети организации (КСО) относятся к распределенным компьютерным системам, осуществляющим автоматизированную обработку информации. Проблема обеспечения информационной безопасности является центральной для таких компьютерных систем. Обеспечение безопасности КСО предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования КСО, а также попыткам модификации, хищения, вывода из строя или разрушения ее компонентов, то есть защиту всех компонентов КСО – аппаратных средств, программного обеспечения, данных и персонала.

Рассмотрим, как в настоящее время обстоит вопрос обеспечения ИБ на предприятии связи. Исследовательская компания Gartner Group выделяет 4 уровня зрелости компании с точки зрения обеспечения информационной безопасности (ИБ):

**0 уровень:**

ИБ в компании никто не занимается, руководство компании не осознает важности проблем ИБ;

Финансирование отсутствует;

ИБ реализуется штатными средствами операционных систем, СУБД и приложений (парольная защита, разграничение доступа к ресурсам и сервисам).

Наиболее типичным примером здесь является компания с небольшим штатом сотрудников, занимающаяся, например, куплей/продажей товаров. Все технические вопросы находятся в сфере ответственности сетевого администратора, которым часто является студент. Здесь главное, что бы все работало.

**1 уровень:**

ИБ рассматривается руководством как чисто "техническая" проблема, отсутствует единая программа (концепция, политика) развития системы обеспечения информационной безопасности (СОИБ) компании;

Финансирование ведется в рамках общего ИТ - бюджета;

ИБ реализуется средствами нулевого уровня + средства резервного копирования, антивирусные средства, межсетевые экраны, средства организации VPN (традиционные средства защиты).

**2 и 3 уровни:**

ИБ рассматривается руководством как комплекс организационных и технических мероприятий, существует понимание важности ИБ для производственных процессов, есть утвержденная руководством программа развития СОИБ компании;

Финансирование ведется в рамках отдельного бюджета;

ИБ реализуется средствами первого уровня + средства усиленной аутентификации, средства анализа почтовых сообщений и web контента, IDS (системы обнаружения вторжений), средства анализа защищенности, SSO (средства однократной аутентификации), PKI (инфраструктура открытых ключей) и организационные меры (внутренний и внешний аудит, анализ риска, политика информационной безопасности, положения, процедуры, регламенты и руководства).

**3 уровень отличается от 2-го следующим:**

ИБ является частью корпоративной культуры, назначен CISA (старший офицер по вопросам обеспечения ИБ);

Финансирование ведется в рамках отдельного бюджета, который согласно результатам исследований аналитической компании Datamonitor в большинстве случаев составляет не более 5% ИТ бюджета;

ИБ реализуется средствами второго уровня + системы управления ИБ, CSIRT (группа реагирования на инциденты нарушения ИБ), SLA (соглашение об уровне сервиса).

Таким образом, серьезный подход к вопросам обеспечения ИБ появляется только на 2-ми 3-м уровнях. А на 1-м и частично 0-м уровне зрелости согласно данной классификации имеет место так называемый «фрагментарный» подход к обеспечению ИБ. «Фрагментарный» подход направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы ит.п.

Достоинство этого подхода заключается в высокой избирательности к конкретной угрозе. Существенным недостатком подхода является отсутствие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечивают защиту конкретных объектов КС только от конкретной угрозы. Даже небольшое вида изменение угрозы ведет к потере эффективности защиты.

Таких компаний по статистике Gartner – 85%.(0 – 30 %, 1 – 55%) по состоянию на 2005.

Более серьезные организации, соответствующие 2-му и 3-му уровням зрелости классификации Gartner, применяют «комплексный» подход к обеспечению ИБ. Этот же подход предлагают и крупные компании, профессионально занимающиеся защитой информации.

Комплексный подход основывается на решении комплекса частных задач по единой программе. Этот подход в настоящее время является основным для создания защищенной среды обработки информации в корпоративных системах, сводящей воедино разнородные меры противодействия угрозам. Сюда относятся правовые, морально этические, организационные, программные и технические способы обеспечения информационной безопасности. Комплексный подход позволил объединить целый ряд автономных систем путем их интеграции в так называемые интегрированные системы безопасности.

Методы решения задач обеспечения безопасности очень тесно связаны с уровнем развития науки и техники и, особенно, с уровнем технологического обеспечения. А характерной тенденцией развития современных технологий является процесс тотальной интеграции. Этой тенденцией охвачены микроэлектроника и техника связи, сигналы и каналы, системы и сети. В качестве примеров можно привести сверхбольшие интегральные схемы, интегральные сети передачи данных, многофункциональные устройства связи ит. п.

Дальнейшим развитием комплексного подхода или его максимальной формой является интегральный подход, основанный на интеграции различных подсистем обеспечения безопасности, подсистем связи в единую интегральную систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных. Интегральный подход направлен на достижение интегральной безопасности. Основной смысл понятия интегральной безопасности состоит в необходимости обеспечить такое состояние условий функционирования корпорации, при котором она надежно защищена от всех возможных видов угроз в ходе всего непрерывного производственного процесса. Понятие интегральной безопасности предполагает обязательную непрерывность процесса обеспечения безопасности, как во времени, так и в пространстве (по всему технологическому циклу деятельности) с обязательным учетом всех возможных видов угроз (несанкционированный доступ, съем информации, терроризм, пожар, стихийные бедствия ит. д.).

В какой бы форме ни применялся комплексный или интегральный подход, он всегда направлен на решение ряда частных задач в их тесной взаимосвязи с использованием общих технических средств, каналов связи, программного обеспечения. Например, применительно к информационной безопасности наиболее очевидными из них являются задачи ограничения доступа к информации, технического и криптографического закрытия информации, ограничения уровней паразитных излучений технических средств, охраны и тревожной сигнализации. Однако необходимо решение и других, не менее важных задач. Так, например, выведение из строя руководителей предприятия, членов их семей или ключевых работников должно поставить под сомнение само существование данного предприятия. Этому же могут способствовать стихийные бедствия, аварии, терроризм и т. п. Поэтому объективно обеспечить полную безопасность информации могут лишь интегральные системы безопасности, индифферентные к виду угроз безопасности и обеспечивающие требуемую защиту непрерывно, как во времени, так и в пространстве, в ходе всего процесса подготовки, обработки, передачи и хранения информации.

## Вопросы информационных безопасности интернет – сервисов

Всемирная паутина World Wide Web

WWW стала одной из основных причин взрывного расширения Интернет в последние годы. Причиной ее популярности стала возможность интерактивного доступа к данным разных типов, в том числе гипертексту, графике, аудио, видео и т.д. World wide web представляет собой множество HTTP-серверов в Интернет.

Проблемы безопасности HTTP-клиентов связаны с их расширяемостью. Поскольку web-серверы предоставляют данные во многих форматах (обычный текст, HTML, графические файлы gif и jpeg, аудио файлы и др.), для воспроизведения различных форматов браузеры вызывают внешние приложения. Например, для просмотра файла формата Microsoft Word, браузер вызовет Microsoft Word. Как правило, браузеры предупреждают пользователя о том, что для открытия файла будет вызвана внешняя программа и требуют подтверждения, и, также как правило, пользователи не обращают внимания на эти предупреждения. При том что многие форматы данных могут включать исполняемый код, как, например, макросы в документах Microsoft Word и Microsoft Excel, простой просмотр с виду безобидных материалов может привести к исполнению произвольного кода на машине пользователя от его имени.

Следует также принимать во внимание существование “активных компонент” (active content), таких как Java-апплеты, Javascript, ActiveX и т.п., которые также содержат код, выполняемый от имени пользователя. Вопросы безопасности “активных компонент” выходят, далеко за рамки данной работы и за их рассмотрением следует обратиться к работе.

Простого решения проблем безопасности, связанных с активными компонентами и другим исполняемым кодом, загружаемым, из www не существует. Методы борьбы с проблемами включают в себя обучение пользователей и объяснение им проблем безопасности, связанных с загружаемым из сети исполняемым кодом, отключение в клиентском программном обеспечении возможности исполнения загружаемых активных компонент, своевременное обновление клиентского ПО для исправления замеченных в нем ошибок и т.п.

Электронная почта

Электронная почта является широко распространенной и интенсивно используемой службой. Сама по себе она представляет сравнительно небольшой риск, но, тем не менее, его следует учитывать.

Основные проблемы, связанные с электронной почтой:

* подделка электронной почты. Протокол SMTP, используемый для передачи электронной почты в Интернет не предоставляет средств аутентификации отправителя. Адрес отправителя письма может быть легко подделан. Подделка электронной почты может использоваться для атак типа "social engineering". Например, пользователь получает письмо якобы от системного администратора с просьбой сменить пароль на указанный в письме.
* передача исполняемого кода в почтовых сообщениях. Электронная почта позволяет передавать данные разных типов, в том числе программы, а также документы, содержащие макросы. Вместе с подделкой адреса отправителя это может использоваться для всевозможных атак. Приведу два примера. Пользователь получает письмо от Santa.Claus@northpole.org, в котором содержится поздравление с Новым Годом и "подарок" - программа, которую предлагается запустить. Запущенная программа рисует на экране, например, новогоднюю елку с мигающей гирляндой. Пользователь пересылает это поздравление всем своим друзьям и знакомым. Программа, рисующая елку, помимо этого инсталлирует программу удаленного управления, и сообщает о результате своему создателю. Второй пример. Системный администратор получает письмо от фирмы - производителя используемого в компании программного обеспечения, с сообщением, что в этом программном обеспечении найдена опасная ошибка и с исправлением, которое следует срочно установить. Результат аналогичен первому примеру.
* перехват почтовых сообщений. Электронная почта передается через Интернет в незашифрованном виде и может быть перехвачена и прочитана.
* Спам. Спамом называется массовая рассылка сообщений рекламного характера. В отличие от обычной рекламы на телевидении или радио, за которую платит рекламодатель, оплата передачи спама ложится на получателя. Обычно спаммеры используют следующую схему: с подключения по коммутируемой линии устанавливается SMTP-соединение с хостом, на котором разрешена пересылка почты на любые хосты (open mail relay - открытый релей). На него посылается письмо со множеством адресатов и, как правило, с поддельным адресом отправителя. Хост, оказавшийся жертвой, пересылает полученное сообщение всем адресатам. В результате, затраты на рассылку спама ложатся на получателей и хост, пересылающий почту. Интернет сервис провайдеры отрицательно относятся к спаму, поскольку он создает весьма существенную нагрузку на их системы и неудобства их пользователям. Поэтому многие провайдеры включают в договор о предоставлении услуг пользователям пункт о недопустимости спама и отключают пользователей, замеченных в рассылке спама. Кроме того, многие провайдеры отключают прием почты с открытых релеев, замеченных в передаче спама. Системному администратору почтового сервера следует убедиться, что его система пересылает исключительно почту, адресованную ее пользователям или исходящую от ее пользователей, чтобы система не могла быть использована спаммерами.
* ошибки в программном обеспечении почтовых серверов. Серверы электронной почты (SMTP, POP3, IMAP) печально известны множеством ошибок, приводившим к взлому систем. Sendmail, один из самых распространенных SMTP-серверов заслужил репутацию самой "дырявой" программы, из когда-либо использовавшихся. За последние два года были также найдены ошибки в распространенном POP3-сервере QUALCOMM qpopper и IMAP-сервере университета Вашингтона, которые позволяют удаленному взломщику получить привилегированный доступ (root) к системе. По сведениям CERT тысячи систем были взломаны благодаря этим ошибкам. Системному администратору следует внимательно следить за сообщениями о найденных ошибках в почтовых серверах и своевременно устанавливать исправленные версии.

FTP - протокол передачи файлов

Протокол FTP используется для передачи файлов. Большинство web-броузеров прозрачно поддерживают FTP. Можно также использовать специальные FTP-клиенты.

Основной проблемой как и в случае www являются программы, выкачиваемые и устанавливаемые пользователями, которые могут носить вредоносный характер.

DNS - доменная система имен

DNS - доменная система имен - производит преобразование имен в адреса и наоборот. Все программы, которые используют для обращения к удаленным хостам имена, являются DNS-клиентами. В этом смысле, практически любая программа, использующая IP-сети, включая web-броузеры, клиентские почтовые программы, FTP-клиенты, и т.п. используют DNS. Таким образом, DNS является основополагающей службой, которую используют другие службы для своей работы.

DNS работает следующим образом: клиент посылает запрос локальному серверу (например, запрашивает IP-адрес www.microsoft.com). Сервер проверяет, есть ли у него эта информация в кэше, и если нет, DNS-сервер запрашивает другие DNS-сервера по очереди, чтобы получить ответ на запрос клиента. Когда DNS-сервер получает ответ, или решает, что ответ получить нельзя, он кэширует полученную информацию и передает ответ клиенту.

Поскольку DNS критична для работы других сервисов, система наделена избыточностью. За каждый участок дерева имен отвечает один первичный (primary) и один и более вторичных (secondary) серверов. Первичный сервер содержит основную копию информации об обслуживаемом участке (зоне). Все изменения в информацию о зоне вносятся на первичном сервере. Вторичные сервера периодически запрашивают "зонную пересылку" (zone transfer) и копируют себе зонную информацию первичного сервера. Таким образом, существует два типа обращений к DNS-серверу - клиентские запросы (lookups) и зонные пересылки (zone transfers).

DNS-сервер использует порт 53. Клиентские запросы используют UDP в качестве транспорта. Если при пересылке клиентского запроса по UDP данные теряются, клиент повторяет запрос по TCP. Для зонных пересылок всегда используется TCP.

Проблемы безопасности DNS:

* Раскрытие информации. DNS может сообщить потенциальному взломщику больше информации, чем следует, например имена и адреса внутренних серверов и рабочих станций.
* DNS spoofing. DNS подвержена атаке, подробно описанной в работе. Вкратце, суть ее в следующем: атакуемый хост разрешает доступ к некоторой своей службе доверяемому хосту с известным именем. Взломщик желает обмануть хост, предоставляющий сервис, представившись ему доверяемым хостом. Для этого взломщику необходимо контролировать обратную зону (преобразующую IP-адреса в имена) к которой относится хост, с которого проводится атака. Прописав в ней соответствие своему IP-адресу имени доверяемого хоста, взломщик получает доступ к сервису, предоставляемому доверяемому хосту. Реализуется следующий сценарий: взломщик устанавливает соединение на атакуемый хост. Атакуемый хост, чтобы убедиться, что запрос исходит от доверяемого хоста, запрашивает у DNS имя по IP-адресу. Поскольку авторитетным сервером для зоны, к которой относится IP-адрес взломщика, является сервер взломщика, запрос адресуется к нему. Он в ответ сообщает имя доверяемого хоста.
* Cache Poisoning. Атака базируется на следующем свойстве: когда один DNS-сервер обращается к другому с запросом, отвечающий сервер, помимо запрашиваемой информации может сообщать дополнительную информацию. Например, если запрашивается MX (mail exchanger) для некоторого домена, отвечающий сервер помимо собственно MX записи передает также A-записи для всех mail exchanger'ов домена. Теперь рассмотрим такую ситуацию: взломщик имеет административный доступ к некоторому DNS-серверу, авторитетному по отношению к какому-нибудь домену. Взломщик модифицирует свой сервер таким образом, что при ответе на запрос об определенной записи, сервер возвращает некоторую дополнительную запись. Взломщик обращается к атакуемому DNS-серверу с запросом о своей особой записи. Сервер обращается с запросом к серверу взломщика, получает дополнительную запись и кэширует ее.
* Ошибки в программном коде DNS-сервера. В 1998 году в широко используемом DNS-сервере BIND было найдено несколько ошибок, одна из которых позволяла получить удаленному взломщику привилегированный (root) доступ к системе. Эти ошибки были исправлены в следующих версиях.

Прочие Интернет - сервисы.

Помимо описанных выше достаточно стандартных служб, существует множество других, более или менее распространенных или используемых. Отмечу основные проблемы, характерные для очень многих из них.

Аутентификация. Большинство электронных информационных сервисов (например, ICQ, IRC) не дает возможности убедиться, что их участники действительно те, за кого себя выдают. Следует очень осторожно относиться к информации, полученной из не аутентифицированного источника.

Передача исполняемого кода. Некоторые информационные службы (ICQ) позволяют пересылать произвольные файлы, в том числе файлы с исполняемым кодом. Исполняемый код, полученный из непроверенного источника может содержать что угодно - вирусы, троянских коней и т.п.

Программные ошибки. Ошибки в программном обеспечении могут приводить к различным проблемам - от отказа в обслуживании до исполнения на машине пользователя злонамеренного программного кода без его согласия и ведома.

## Методы защиты компьютерной сети организации от НСД из сети Интернет. Применение межсетевых экранов

Существует несколько подходов к решению проблемы защиты КСО подключенной к сети Интернет от НСД. Первый подход состоит в усилении защиты всех имеющихся систем, открытых к доступу из Интернет. Этот подход называется "безопасность на уровне хоста". Он может включать в себя обучение пользователей и администраторов систем работе в более недружелюбной среде, ужесточение политики парольной защиты (введение или ужесточение ограничений на минимальную длину, символьный состав и срок действия пароля) или введение не парольных методов аутентификации, ужесточение правил доступа к системам, ужесточение требований к используемому программному обеспечению, в том числе операционным системам, и регулярная проверка выполнения всех введенных требований.

У этого подхода есть несколько недостатков:

* для пользователей усложняются процедуры работы в системе, и возможно, некоторые действия к которым они привыкли, вообще запрещены. Это может привести к снижению производительности пользователей, а также к их недовольству.
* на администраторов системы ложится очень существенная дополнительная нагрузка по поддержке системы. Даже для сравнительно небольших систем, содержащих несколько десятков машин, задача поддержания заданного уровня безопасности может потребовать непропорционально больших усилий.
* требования защиты могут, противоречить требованиям использования системы и одним из них придется отдать предпочтение в ущерб другим. Как правило, требованиям к функциональности системы отдается предпочтение в ущерб требования защиты.

Достоинством этого подхода является то, что помимо проблемы защиты от "внешнего врага" он также решает проблему внутренней безопасности системы. Поскольку значительная часть инцидентов (по некоторым данным до 80%), связанных с безопасностью, исходит от сотрудников или бывших сотрудников компаний, этот подход может весьма эффективно повысить общую безопасность системы.

Второй подход является наиболее радикальным. В нем рабочая сеть компании физически не соединена с Интернет. Для взаимодействия с Интернет используется одна или несколько специально выделенных машин, не содержащих никакой конфиденциальной информации. Достоинства этого подхода очевидны: поскольку рабочая сеть не соединена с Интернет, угроза НСД из сети Интернет для нее отсутствует в принципе. В то же время, этот подход имеет определенные ограничения и недостатки. Ограничением, во определенных случаях приемлемым, является отсутствие доступа к Интернет с рабочих мест сотрудников. Недостатки этого подхода проистекают из наличия незащищенных систем, подключенных к Интернет, которые могут подвергаться атакам типа "отказ в обслуживании", и краже услуг (в том числе могут быть использованы для взлома других систем). Вариацией этого подхода является разграничение по протоколам. Например, для доступа к информационным ресурсам компании используется стек протоколов IPX/SPX, а для доступа в Интернет - TCP/IP. При этом, например, серверы Novell Netware, будут невидимы для взломщика и не могут быть атакованы напрямую из Интернет. Этот подход также имеет определенные ограничения. Например, он неприемлем для сети, в которой необходимо использование TCP/IP для доступа к внутренним ресурсам. Вторым его недостатком является то, что пользовательские системы видимы и доступны из Интернет и могут быть использованы как плацдарм для последующей атаки на серверы.

Третий подход, называемый "безопасность на уровне сети" состоит в введении средств ограничения доступа в точке соединения сетей. Этот подход позволяет сконцентрировать средства защиты и контроля в точках соединения двух и более сетей, например в точке соединения КСО с Интернет. В этой точке находится специально выделенная система - межсетевой экран - которая и осуществляет контроль за информационным обменом между двумя сетями и фильтрует информацию в соответствии с заданными правилами, определяемыми политикой безопасности компании. Весь обмен данными, происходящий между сети Интернет и внутренней сетью, проходит через межсетевой экран. Организация может получить значительный выигрыш от такой модели безопасности. Единственная система, выполняющая роль межсетевого экрана, может защитить от несанкционированного доступа десятки и сотни систем, скрытых за ней, без наложения на них дополнительных требований к безопасности. Достоинствами этого подхода является концентрация средств защиты и контроля в одной точке, минимальное изменение внутренних процедур работы пользователей с информационной системой, сравнительно большая простота администрирования и возможно больший уровень защиты. Ограничением этого подхода является то, что он предназначен исключительно для защиты от внешних угроз, исходящих от удаленных взломщиков.

Рассмотрим теперь типичную КСО с точки зрения применимости к ней вышеописанных методов защиты. Как правило, она состоит из клиентских компьютеров под управлением Microsoft Windows XP или реже Windows NT Workstation, серверов Microsoft Windows NT Server, Novell Netware и/или различных Unix-систем, и, возможно, другого сетевого оборудования, такого как сетевые принтеры, концентраторы, коммутаторы и маршрутизаторы с возможностью удаленного управления и т.п.

Использование исключительно модели безопасности на уровне хоста в этом случае может быть неприемлемым, по причине большой сложности (а возможно и невыполнимости) доведения уровня защиты используемых систем до необходимого уровня. Проблемы безопасности в сетях на базе систем Microsoft были показаны выше. В случае, если использование для доступа к Интернет физически отделенной от основной сети системы неприемлемо, наиболее эффективным решением является использование технологии межсетевых экранов.

Согласно определению Государственной Технической Комиссии при Президенте Российской Федерации “Межсетевой экран представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и/или выходящей из автоматизированной системы, и обеспечивает защиту автоматизированной системы посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) автоматизированную систему”. Межсетевые экраны, при правильном их использовании, являются весьма эффективным средством защиты от угроз корпоративным сетям, исходящим из сети Интернет.

# 2. Теоретические вопросы построения межсетевых экранов

##

## 2.1 Архитектуры межсетевых экранов

Межсетевое экраны могут быть сконфигурированы в виде одной из нескольких архитектур, что обеспечивает различные уровни безопасности при различных затратах на установку и поддержание работоспособности. Организации должны проанализировать свой профиль риска и выбрать соответствующую архитектуру. Ниже описываются типичные архитектуры межсетевого экрана и приводят примеры политик безопасности для них.

Хост, подключенный к двум сегментам сети

Это такой хост, который имеет более одного интерфейса с сетью, причем каждый интерфейс с сетью подключен физически к отдельному сегменту сети. Самым распространенным примером является хост, подключенный к двум сегментам.

Межсетевой экран на основе хоста, подключенного к двум сегментам сети - это межсетевой экран с двумя сетевыми платами, каждая из которых подключена к отдельной сети. Например, одна сетевая плата соединена с внешней или небезопасной сетью, а другая - с внутренней или безопасной сетью. В этой конфигурации ключевым принципом обеспечения безопасности является запрет прямой маршрутизации трафика из не доверенной сети в доверенную – межсетевой экран всегда должен быть при этом промежуточным звеном.

Маршрутизация должна быть отключена на межсетевом экране такого типа, чтобы IP-пакеты из одной сети не могли пройти в другую сеть.

Такая конфигурация, наверное, является одной из самых дешевых и распространенных при коммутируемом подключении ЛВС организации к сети Интернет. Берется машина, на которую устанавливается FreeBSD, и на ней запрещается маршрутизация, кроме того соответствующим образом конфигурируется встроенный в ядро пакетный фильтр (ipfw).

Экранированный хост

При архитектуре типа экранированный хост используется хост (называемый хостом-бастионом), с которым может установить соединение любой внешний хост, но запрещен доступ ко всем другим внутренним, менее безопасным хостам. Для этого фильтрующий маршрутизатор конфигурируется так, что все соединения с внутренней сетью из внешних сетей направляются к хосту-бастиону.

Если шлюз с пакетной фильтрацией установлен, то хост-бастион должен быть сконфигурирован так, чтобы все соединения из внешних сетей проходили через него, чтобы предотвратить прямое соединение между компьютерной сетью организации и сети Интернет.

Экранированная подсеть

Архитектура экранированной сети по существу совпадает с архитектурой экранированного хоста, но добавляет еще одну линию защиты, с помощью создания сети, в которой находится хост-бастион, отделенной от внутренней сети.

Экранированная подсеть должна внедряться с помощью добавления сети-периметра для того, чтобы отделить внутреннюю сеть от внешней. Это гарантирует, что даже при успехе атаки на хост-бастион, атакующий не сможет пройти дальше сети-периметра из-за того, что между внутренней сетью и сетью-периметром находится еще один экранирующий маршрутизатор.

## 2.2 Классификация межсетевых экранов

Межсетевые экраны являются устройствами или системами, которые управляют потоком сетевого трафика между сетями с различными требованиями к безопасности. В большинстве современных приложений межсетевые экраны и их окружения обсуждаются в контексте соединений в Интернете и, следовательно, использования стека протоколов TCP/IP. Однако межсетевые экраны применяются и в сетевых окружениях, которые не требуют обязательного подключения к Интернету. Например, многие корпоративные сети предприятия ставят межсетевые экраны для ограничения соединений из и во внутренние сети, обрабатывающие информацию разного уровня чувствительности, такую как бухгалтерская информация или информация о заказчиках. Ставя межсетевые экраны для контроля соединений с этими областями, организация может предотвратить неавторизованный доступ к соответствующим системам и ресурсам внутри чувствительных областей. Тем самым, использование межсетевого экрана обеспечивает дополнительный уровень безопасности, который иначе не может быть достигнут.

В настоящее время существует несколько типов межсетевых экранов. Одним из способов сравнения их возможностей является перечисление уровней модели OSI, которые данный тип межсетевого экрана может анализировать- Модель OSI является абстракцией сетевого взаимодействия между компьютерными системами и сетевыми устройствами. Рассмотрим только уровни модели OSI относящиеся к межсетевым экранам. На рис. 2.1 показана стек протоколов модели OSI.

* Сеансовый

Шлюз сеансового уровня

* Уровень 5
* Канальный

Мостиковый экран

* Уровень 2
* Прикладной

Шлюз прикладного уровня

* Уровень 7
* Представительский
* Уровень 6
* Сетевой
* Уровень 3
* Транспортный

Фильтрующий маршрутизатор

* Уровень 4
* Физический
* Уровень 1

Рис.2.1. Стек протоколов модели OSI

Уровень 1 представляет собой реальную аппаратуру физического соединения и среду, такую как Ethernet.

Уровень 2 — уровень, на котором сетевой трафик передается по локальной сети (LAN). Он также является первым уровнем, обладающим возможностью адресации, с помощью которой можно идентифицировать отдельную машину. Адреса назначаются на сетевые интерфейсы и называются MAC (Media Access Control) адресами. Ethernet - адрес, принадлежащий Ethernet-карте, является примером МАС - адреса уровня 2.

Уровень 3 является уровнем, отвечающим за доставку сетевого трафика по WAN. В Интернете адреса уровня 3 называются IP-адресами; адреса обычно являются уникальными, но при определенных обстоятельствах, например, при трансляции сетевых адресов (NAT) возможны ситуации, когда различные физические системы имеют один и тот же IP-адрес уровня 3.

Уровень 4 идентифицирует конкретное сетевое приложение и коммуникационную сессию в дополнение к сетевым адресам; система может иметь большое число сессий уровня 4 с другими ОС. Терминология, связанная с семейством протоколов TCP/IP, включает понятие портов, которые могут рассматриваться как конечные точки сессий: номер порта источника определяет коммуникационную сессию на исходной системе; номер порта назначения определяет коммуникационную сессию системы назначения. Более высокие уровни (5, 6 и 7) представляют приложения и системы конечного пользователя.

Мостиковые межсетевые экраны

Данный класс межсетевого экрана, функционирующий на 2-м уровне модели OSI, известен также как прозрачный (stealth), скрытый, теневой межсетевой экран.

Мостиковые межсетевые экраны появились сравнительно недавно и представляют перспективное направление развития технологий межсетевого экранирования. Фильтрация трафика ими осуществляется на канальном уровне, т.е. межсетевые экраны работают с фреймами (frame, кадр).

К достоинствам подобных межсетевых экранов можно отнести:

• Нет необходимости в изменении настроек корпоративной сети, не требуется дополнительного конфигурирования сетевых интерфейсов межсетевого экрана.

• Высокая производительность. Поскольку это простые устройства, они не требуют больших затрат ресурсов. Ресурсы требуются либо для повышения возможностей машин, либо для более глубокого анализа данных.

• Прозрачность. Ключевым для этого устройства является его функционирование на 2 уровне модели OSI. Это означает, что сетевой интерфейс не имеет IP-адреса. Эта особенность более важна, чем легкость в настройке. Без IP-адреса это устройство не доступно в сети и является невидимым для окружающего мира. Если такой межсетевой экран недоступен, то как его атаковать? Атакующие даже не будут знать, что существует межсетевой экран, проверяющий каждый их пакет.

Фильтрующие маршрутизаторы

Межсетевой экран с фильтрацией пакетов (Packet - filtering firewall) - межсетевой экран, который является маршрутизатором или компьютером, на котором работает программное обеспечение, сконфигурированное таким образом, чтобы отфильтровывать определенные виды входящих и исходящих пакетов. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- IP-заголовках пакетов (адреса отправителя и получателя, их номера портов и др.)

* Работают на 3 уровне
* Также известны, как межсетевой экран на основе порта
* Каждый пакет сравнивается со списками правил (адрес источника/получателя, порт источника/получателя)
* Недорогой, быстрый (производительный в силу простоты), но наименее безопасный
* Технология 20-летней давности
* Пример: список контроля доступа (ACL, access control lists) маршрутизатора

Шлюз сеансового уровня

Шлюз сеансового уровня (Circuit-level gateway) — межсетевой экран, который исключает прямое взаимодействие между авторизированным клиентом и внешним хостом. Сначала он принимает запрос доверенного клиента на определенные услуги и, после проверки допустимости запрошенного сеанса, устанавливает соединение с внешним хостом. На рис. 2.2 показано схема функционирование шлюза сеансового уровня.

Рис. 2.2. Схема функционирование шлюза сеансового уровня

После этого шлюз просто копирует пакеты в обоих направлениях, не осуществляя их фильтрации. На этом уровне появляется возможность использования функции сетевой трансляции адресов (NAT, network address translation). Трансляция внутренних адресов выполняется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов IP-адреса компьютеров - отправителей внутренней сети автоматический преобразуются в один IP-адрес, ассоциируемый с экранирующим межсетевым экраном. В результате все пакеты, исходящие из внутренней сети, оказываются отправленными межсетевым экраном, что исключает прямой контакт между внутренней и внешней сетью. IP-адрес шлюза сеансового уровня становится единственным активным IP-адресом, который попадает во внешнюю сеть.

* Работает на 4 уровне
* Передает TCP подключения, основываясь на порте
* Недорогой, но более безопасный, чем фильтр пакетов
* Вообще требует работы пользователя или программы конфигурации для полноценной работы
* Пример: SOCKS межсетевой экран

Шлюз прикладного уровня

Шлюз прикладного уровня (Application-level gateways) - межсетевой экран, который исключает прямое взаимодействие между авторизированным клиентом и внешним хостом, фильтруя все входящие и исходящие пакеты на прикладном уровне модели OSI. На рис. 2.3 показано функционирование шлюза прикладного уровня.

Рис.2.3. Схема функционирование шлюза прикладного уровня

Связанные с приложением программы-посредники перенаправляют через шлюз информацию, генерируемую конкретными сервисами TCP/IP.

Возможности:

• Идентификация и аутентификация пользователей при попытке установления соединения через межсетевой экран;

• Фильтрация потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;

• Регистрация событий и реагирование на события;

• Кэширование данных, запрашиваемых из внешней сети.

На этом уровне появляется возможность использования функций посредничества (Proxy).

Для каждого обсуживаемого протокола прикладного уровня можно вводить программных посредников – HTTP-посредник, FTP-посредник и т.д. Посредник каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе. Также, как и шлюз сеансового уровня, прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и сходящие пакеты, копирует и перенаправляет информацию через шлюз, и функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью. Однако, посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями программными серверами), а во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели МВОС.

Особенности:

* Работает на 7 уровне;
* Специфический для приложений;
* Умеренно дорогой и медленный, но более безопасный и допускает регистрацию деятельности пользователей;
* Требует работы пользователя или программы конфигурации для полноценной работы;
* Пример: Web (http) proxy;

Стек протоколов TCP/IP соотносится с уровнями модели OSI следующим образом:

* Транспортный

TCP - сессии

* Уровень 4
* Сетевой

IP-адресация

* Уровень 3
* Канальный

Ethernet-адресация

* Уровень 2
* Прикладной

Почтовые клиенты, web-браузеры

* Уровень 7

Рис. 2.4. Взаимосвязь уровней стека протоколов ТСР/IР и OSI

Современные межсетевые экраны функционируют на любом из перечисленных уровней. На рис. 2.4 показано взаимосвязь уровней стека протоколов TCP/IP и OSI. Первоначально межсетевые экраны анализировали меньшее число уровней; теперь более мощные из них охватывают большее число уровней. С точки зрения функциональности, межсетевой экран, имеющий возможность анализировать большее число уровней, является более совершенным и эффективным. За счет охвата дополнительного уровня также увеличивается возможность более тонкой настройки конфигурации межсетевого экрана. Возможность анализировать более высокие уровни позволяет межсетевого экрана предоставлять сервисы, которые ориентированы на пользователя, например, аутентификация пользователя. Межсетевой экран, который функционирует на уровнях 2, 3 и 4, не имеет дело с подобной аутентификацией.

Независимо от архитектуры межсетевой экран может иметь дополнительные сервисы. Эти сервисы включают трансляцию сетевых адресов (NAT), поддержку протокола динамической конфигурации хоста (DHCP) и функции шифрования, тем самым являясь конечной точкой VPN-шлюза, и фильтрацию на уровне содержимого приложения.

Многие современные межсетевые экраны могут функционировать как VPN-шлюзы. Таким образом, организация может посылать незашифрованный сетевой трафик от системы, расположенной позади межсетевого экрана, к удаленной системе, расположенной позади корпоративного VPN-шлюза; межсетевой экран зашифрует трафик и перенаправит его на удаленный VPN-шлюз, который расшифрует его и передаст целевой системе. Большинство наиболее популярных межсетевых экранов сегодня совмещают эти функциональности.

Многие межсетевые экраны также включают различные технологии фильтрации активного содержимого. Данный механизм отличается от обычной функции межсетевого экрана тем, что межсетевой экран теперь также имеет возможность фильтровать реальные прикладные данные на уровне 7, которые проходят через него. Например, данный механизм может быть использован для сканирования на предмет наличия вирусов в файлах, присоединенных к почтовому сообщению. Он также может применяться для фильтрации наиболее опасных технологий активного содержимого в web, таких как Java, JavaScript и ActiveX. Или он может быть использован для фильтрации содержимого или ключевых слов с целью ограничения доступа к неподходящим сайтам или доменам. Тем не менее, компонент фильтрации, встроенный в межсетевой экран, не должен рассматриваться как единственно возможный механизм фильтрации содержимого; возможно применение аналогичных фильтров при использовании сжатия, шифрования или других технологий.

## 2.3 Различные типы окружений межсетевых экранов

Окружение межсетевого экрана является термином, который применяется для описания множества систем и компонент, используемых для поддержки функционирования межсетевого экрана в конкретной сети. Простое окружение межсетевого экрана может состоять только из пакетного фильтра. В более сложном и безопасном окружении оно состоит из нескольких межсетевых экранов и прокси со специальной топологией. Рассмотрим возможные сетевые топологии, используемые в качестве окружений межсетевого экрана.

Принципы построения окружения межсетевых экранов

Существует четыре принципа, которым необходимо следовать:

1. Простота (Keep It Simple)

Данный принцип говорит о первом и основном, о чем надо помнить при разработки топологии сети, в которой функционирует межсетевой экран. Важно принимать наиболее простые решения — более безопасным является то, чем легче управлять. Трудно понимаемые функциональности часто приводят к ошибкам в конфигурации.

1. Использование устройств по назначению

Использование сетевых устройств для того, для чего они первоначально предназначались, в данном контексте означает, что не следует делать межсетевые экраны из оборудования, которое не предназначено для использования в качестве межсетевого экрана. Например, роутеры предназначены для рейтинга; возможности фильтрования пакетов не являются их исходной целью, и это всегда надо учитывать при разработке окружения межсетевого экрана. Зависимость исключительно от возможности роутера обеспечивать функциональность межсетевого экрана опасна: он может быть легко переконфигурирован. Другим примером являются сетевые коммуникаторы (switch): когда они используются для обеспечения функциональности межсетевого экрана вне окружения межсетевого экрана, они чувствительны к атакам, которые могут нарушить функционирование коммуникатора. Во многих случаях гибридные межсетевые экраны и устройства межсетевых экранов являются лучшим выбором, потому что они оптимизированы в первую очередь для функционирования в качестве межсетевых экранов.

3. Создание обороны вглубь

Оборона вглубь означает создание нескольких уровней защиты в противоположность наличию единственного уровня. Не следует всю защиту обеспечивать исключительно межсетевым экраном. Там, где может использоваться несколько межсетевых экранов, они должны использоваться. Там, где роутеры могут быть сконфигурированы для предоставления некоторого управления доступом или фильтрации, это следует сделать. Если ОС сервера может предоставить некоторые возможности межсетевого экрана, это следует применить.

4. Внимание к внутренним угрозам

Наконец, если уделять внимание только внешним угрозам, то это приводит в тому, что сеть становится открытой для атак, изнутри. Хотя это и маловероятно, но следует рассматривать возможность того, что нарушитель может как-то обойти межсетевой экран и получить свободу действий для атак внутренних или внешних систем. Следовательно, важные системы, такие как внутренние web или e-mail серверы или финансовые системы, должны быть размещены позади внутренних межсетевых экранов или DMZ-зон.

В качестве итога заметим, что выражение «всю защиту можно взломать» особенно применимо к построению окружений межсетевого экрана. При развертывании межсетевых экранов следует помнить о перечисленных выше правилах для определения окружений, но в каждом случае могут иметь место свои собственные требования, возможно, требующие уникальных решений.

DMZ – сети

В большинстве случаев окружение межсетевого экрана образует так называемую DMZ-сеть или сеть демилитаризованной зоны. DMZ-сеть является сетью, расположенной между двумя межсетевыми экранами.

Конфигурация с одной DMZ-сетью

DMZ-сети предназначены для расположения систем и ресурсов, которым необходим доступ либо только извне, либо только изнутри, либо и извне, и изнутри, но которые не должны быть размещены во внутренних защищенных сетях. Причина в том, что никогда нельзя гарантировать, что эти системы и ресурсы не могут быть взломаны. Но взлом этих систем не должен автоматически означать доступ ко всем внутренним системам. Пример окружения межсетевого экрана с одной DMZ показано на рис. 2.5.

Пакетный фильтр пограничного роутера

Основной межсетевой экран

HTTP - сервер

SMTP - сервер

DMZ-сеть

Локальная защищенная сеть

Интернет

Рис. 2.5. Пример окружения межсетевого экрана с одной DMZ

DMZ-сети обычно строятся с использованием сетевых коммутаторов и располагаются между двумя межсетевыми экранами или между межсетевым экраном и пограничным роутером. Хорошей практикой является размещение серверов удаленного доступа и конечных точек VPN в DMZ-сетях. Размещение этих систем в DMZ-сетях уменьшает вероятность того, что удаленные атакующие будут иметь возможность использовать эти серверы в качестве точки входа в локальные сети. Кроме того, размещение этих серверов в DMZ-сетях позволяет межсетевым экранам служить дополнительными средствами для контроля прав доступа пользователей, которые получают доступ с использованием этих систем к локальной сети.

Service Leg конфигурация

Одной из конфигураций DMZ-сети является так называемая «Service Leg» конфигурация межсетевого экрана на рис. 2.6. В этой конфигурации межсетевой экран создается с тремя сетевыми интерфейсами. Один сетевой интерфейс соединяется с Интернетом, другой сетевой интерфейс соединяется с внутренней сетью, и третий сетевой интерфейс формирует DMZ-сеть. Такая конфигурация может привести к возрастанию риска для межсетевого экрана при деградации сервиса в течение DoS-атаки, которая будет нацелена на сервисы, расположенные в DMZ-сети. В стандартной конфигурации DMZ-сети DoS-атака для присоединенного к DMZ-ресурса, такого как web-сервер, будет соответствующим образом воздействовать только на этот целевой ресурс. В Service Leg конфигурации DMZ-сети межсетевой экран берет на себя основной удар от DoS-атаки, потому что он должен проверять весь сетевой трафик перед тем, как трафик достигнет присоединенного к DMZ - ресурса. Это может влиять на весь трафик организации, если на ее web-сервер выполнена DoS-атака.

Рис. 2.6. Конфигурация Service Leg DMZ

Основной межсетевой экран

Внешняя DMZ-сеть или Интернет

Service Leg DMZ-сеть

Прикладные серверы

Защищенная внутренняя сеть

Конфигурация с двумя DMZ-сетями

При наличии большого числа серверов с разными требованиями доступа можно иметь межсетевой экран пограничного роутера и два внутренних межсетевого экрана разместить все внешне доступные серверы во внешней DMZ между роутером и первым межсетевым экраном. Пограничный роутер будет фильтровать пакеты и обеспечивать защиту серверов, первый межсетевой экран будет обеспечивать управление доступом и защиту от серверов внутренней DMZ в случае, если они атакованы. Организация размещает внутренне доступные серверы во внутренней DMZ, расположенной между основным и внутренним межсетевыми экранами; межсетевые экраны будут обеспечивать защиту и управление доступом для внутренних серверов, защищенных как от внешних, так и от внутренних атак.

Окружение межсетевого экрана для данной сети показано на рис.2.7.

* Внешняя DMZ-сеть соединена с Интернетом через пакетный фильтр, служащий пограничным роутером, - выше были указаны причин, по которым использование пакетного фильтра является предпочтительным.
* Основной межсетевой экран является VPN-шлюзом для удаленных пользователей; такие пользователи должны иметь ПО VPN-клиента для соединения с межсетевым экраном.
* Входящий SMTP-трафик должен пропускаться основным межсетевым экраном.
* Исходящий HTTP-трафик должен проходить через внутренний межсетевой экран, который передает данный HTTP-трафик прикладному НТТР-прокси, размещенному во внутренней DMZ.

Основные и внутренние межсетевые экраны должны поддерживать технологию stateful inspection и могут также включать возможности прикладного прокси. Основной межсетевой экран должен выполнять следующие действия:

* разрешать внешним пользователям соединяться с VPN-сервером, где они должны аутентифицироваться;
* пропускать внутренние SMTP-соединения и данные к прокси-серверу, где данные могут быть отфильтрованы и переданы системам назначения;
* выполнять роутинг исходящего HTTP-трафика от HTTP-прокси и исходящего SMTP-трафика от SMTP-сервера;
* после этого запретить весь другой исходящий HTTP- и SMTP-трафик;
* после этого разрешить весь другой исходящий трафик;

Внутренний межсетевой экран должен принимать входящий трафик только от основного межсетевого экрана, прикладного HTTP-прокси и SMTP-сервера. Кроме того, он должен принимать SMTP- и HTTP-трафик только от прокси, но не от основного межсетевого экрана. Наконец, он должен разрешать все исходящие соединения от внутренних систем.

Чтобы сделать данный пример применимым к окружениям с более высокими требованиями к безопасности, можно добавить следующие сервисы:

* могут быть добавлены внутренний и внешний DNS-серверы, чтобы спрятать внутренние системы;
* может попользоваться NAT для дальнейшего сокрытия внутренних систем;
* исходящий трафик от внутренних систем может фильтроваться, что может включать фильтрование трафика к определенным сайтам или сервисам в соответствии с политикой управления;
* может быть использовано несколько межсетевых экранов для увеличения производительности;

 Рис.2.7. Пример окружения межсетевого экрана с двумя DMZ-сетями

Пограничный роутер с возможностями пакетного фильтра

Интернет

Внешняя DMZ-сеть

Dial-in сервер

Внешний HTTP-сервер

Основной межсетевой экран VPN Gateway

Внешняя DMZ-сеть

Внутренний межсетевой экран

HTTP прокси - сервер

SMTP -сервер

Локальная защищенная сеть

Интранет

Интранет является сетью, которая выполняет те же самые сервисы, приложения и протоколы, которые присутствуют в Интернете, но без наличия внешнего соединения с Интернетом. Например, сеть предприятии, поддерживающая семейство протоколов TCP/IP, можно рассматривать как Интранет.

Большинство организаций в настоящее время имеет некоторый тип Интранета. Во внутренней сети (интранет) могут быть созданы еще меньшие Интранеты, используя внутренние межсетевые экраны. Например, можно защитить свою собственную персональную сеть внутренним межсетевым экраном, и получившаяся защищенная сеть может рассматриваться как персональная интранет.

Так как Интранет использует те же самые протоколы и прикладные сервисы, что и Интернет, многие проблемы безопасности, унаследованные из Интернета, также присутствуют в Интранете.

Экстранет

Термин «Экстранет» применяется к сети, логически состоящей из трех частей: две интранет соединены между собой через Интернет с использованием VPN. Экстранет может быть определена как business-to-business Интранет. Эта сеть позволяет обеспечить ограниченный, управляемый доступ удаленных пользователей посредством той же формы аутентификации и шифрования, которые имеются в VPN.

Экстранет имеет те же самые характеристики, что и интранет, за исключением того, что экстранет использует VPN для создания защищенных соединений через публичный Интернет. Целью интранет является предоставление доступа к потенциально чувствительной информации удаленным пользователям или организациям, но при этом запрещая доступ всем остальным внешним пользователям и системам. Экстранет использует протоколы TCP/IP и те же самые стандартные приложения и сервисы, которые используются в Интернете. На рис. 2.8 показан пример топологии сети экстранет.

Межсетевой экран А

Межсетевой экран В

Защищенная сеть интранет А

Интернет

Интернет

VPN

Экстранет

Защищенная сеть интранет В

Рис.2.8. VPN и экстранет, соединяющие две сети Интранета

Компоненты инфраструктуры: концентраторы и коммутаторы

Дополнительно к роутерам и межсетевым экранам, связь между системами обеспечивают такие инфраструктурные устройства, как концентраторы (hubs) и коммутаторы (switches). Наиболее простым из них является сетевой концентратор. Концентраторы — это устройства, которые функционируют на уровне 1 модели OSI. Другими словами, они предназначены только для предоставления физического подсоединения сетевых систем или ресурсов.

У сетевых концентраторов существует много слабых мест. Первое и основное состоит в том, что концентраторы позволяют любому устройству, присоединенному к ним, просматривать весь сетевой трафик. По этой причине они не должны использоваться для построения DMZ-сетей или окружений межсетевого экрана.

Более развитыми инфраструктурными устройствами являются сетевые коммутаторы. Это устройства уровня 2, то есть они обладают определенной информацией при создании присоединения сетевых систем или компонент.

Основное свойство коммутаторов состоит в том, что системы, присоединенные к коммутатору, не могут «подсматривать» трафик друг друга; поэтому они лучше подходят для реализации DMZ-сетей и окружений межсетевых экранов.

Важно заметить, что коммутаторы не должны использоваться для предоставления каких-либо возможностей межсетевого экрана или обеспечения изолирования трафика вне окружения межсетевого экрана, так как при этом возможны DoS-атаки, которые могут привести к тому, что коммутаторы переполнят присоединенные сети пакетами.

## 2.4 Уровень защищенности межсетевых экранов

В соответствии с уровень защищенности межсетевых экранов оценивается по следующим показателям:

1. Управление доступом (фильтрация данных и трансляция адресов)
2. Идентификация и аутентификация
3. Регистрация
4. Администрирование: идентификация и аутентификация
5. Администрирование: регистрация
6. Администрирование: простота использования
7. Целостность
8. Восстановление
9. Тестирование
10. Руководство администратора защиты
11. Тестовая документация
12. Конструкторская (проектная) документация

Для каждого класса защищенности определяются требования к указанным показателям.

Далее следуют требования к межсетевому экрану в соответствии с документом Государственной Технической Комиссии по межсетевым экранам для пятого и четвертого класса защищенности и описание уровня соответствия этим требованиям.

1. Управление доступом.

Требования к пятому классу:

*Межсетевой экран должен обеспечивать фильтрацию на сетевом уровне. Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов.*

Требования к четвертому классу:

*Данные требования полностью включают аналогичные требования пятого класса. Дополнительно межсетевой экран должен обеспечивать:*

* *фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;*
* *фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;*
* *фильтрацию с учетом любых значимых полей сетевых пакетов.*

Требования к третьему классу:

*Данные требования полностью включают аналогичные требования четвертого класса.*

*Дополнительно межсетевой экран должен обеспечивать:*

* *фильтрацию на транспортном уровне запросов на установление виртуальных соединений. При этом, по крайней мере, учитываются транспортные адреса отправителя и получателя;*
* *фильтрацию на прикладном уровне запросов к прикладным сервисам. При этом, по крайней мере, учитываются прикладные адреса отправителя и получателя;*
* *фильтрацию с учетом даты/времени.*
1. Идентификация и аутентификация

Нет требований к четвертому и пятому классу. Требования к третьему классу:

*Межсетевой экран должен обеспечивать возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.*

1. Регистрация

Нет требований к пятому классу. Требования к четвертому классу:

*Межсетевой экран должен обеспечивать возможность регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.*

Требования к третьему классу:

*Данные требования включают аналогичные требования четвертого класса.*

*Дополнительно межсетевой экран должен обеспечивать:*

* *регистрацию и учет запросов на установление виртуальных соединений;*
* *локальную сигнализацию попыток нарушения правил фильтрации.*
1. Администрирование: идентификация и аутентификация

Требования к пятому классу:

*Межсетевой экран должен обеспечивать идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ. Межсетевой экран должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.*

Требования к четвертому классу:

*Данные требования полностью совпадают с аналогичными требованиями пятого класса.*

Требования к третьему классу:

*Данные требования включают аналогичные требования пятого класса. Дополнительно межсетевой экран должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась. При удаленных запросах администратора межсетевого экрана на доступ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.*

1. Администрирование: регистрация

Требования к пятому классу:

*Межсетевой экран должен обеспечивать регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузка и инициализация системы и ее программный останов. Регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана;*

*В параметрах регистрации указываются:*

* *дата, время и код регистрируемого события;*
* *результат попытки осуществления регистрируемого события - успешная или неуспешная;*
* *идентификатор администратора межсетевого экрана, предъявленный при попытке осуществления регистрируемого события.*

Требования к четвертому классу:

*Данные требования включают аналогичные требования пятого класса.*

*Дополнительно межсетевой экран должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).*

Требования к третьему классу:

*Данные требования полностью включают аналогичные требования четвертого класса.*

*Дополнительно межсетевой экран должен обеспечивать регистрацию действия администратора межсетевого экрана по изменению правил фильтрации.*

1. Администрирование: простота использования

Нет требований к четвертому и пятому классу. Требования к третьему классу:

*Многокомпонентный межсетевой экран должен обеспечивать возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.*

1. Целостность

Требования к пятому классу:

*Межсетевой экран должен содержать средства контроля над целостностью своей программной и информационной части.*

Требования к четвертому классу:

*Данные требования полностью совпадают с аналогичными требованиями пятого класса.*

Требования к третьему классу:

*Данные требования полностью включают аналогичные требования пятого класса.*

*Дополнительно должен обеспечиваться контроль целостности программной и информационной части межсетевого экрана по контрольным суммам.*

1. Восстановление

Требования к пятому классу:

*Межсетевой экран должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств межсетевого экрана.*

Требования к четвертому классу:

*Данные требования полностью совпадают с аналогичными требованиями пятого класса.*

Требования к третьему классу:

*Данные требования полностью совпадают с аналогичными требованиями пятого класса.*

1. Тестирование

Требования к пятому классу:

*В межсетевом экране должна обеспечиваться возможность регламентного тестирования:*

* *реализации правил фильтрации;*
* *процесса идентификации и аутентификации администратора;*
* *процесса регистрации действий администратора межсетевого экрана;*
* *процесса контроля за целостностью программной и информационной части межсетевого экрана;*
* *процедуры восстановления.*

Требования к четвертому классу:

*В межсетевом экране должна обеспечиваться возможность регламентного тестирования:*

* *реализации правил фильтрации;*
* *процесса регистрации;*
* *процесса идентификации и аутентификации администратора межсетевого экрана;*
* *процесса регистрации действий администратора межсетевого экрана;*
* *процесса контроля за целостностью программной и информационной части межсетевого экрана;*
* *процедуры восстановления.*

Требования к третьему классу:

*В межсетевом экранированием должна обеспечиваться возможность регламентного тестирования*

* *реализации правил фильтрации;*
* *процесса регистрации;*
* *процесса идентификации и аутентификации запросов;*
* *процесса идентификации и аутентификации администратора межсетевого экрана;*
* *процесса регистрации действий администратора межсетевого экрана;*
* *процесса контроля за целостностью программной и информационной части межсетевого экрана;*
* *процедуры восстановления.*
1. Руководство администратора защиты

Требования к пятому классу:

Документ содержит:

* *описание контролируемых функций межсетевого экрана;*
* *руководство по настройке и конфигурированию межсетевого экрана;*
* *описание старта межсетевого экрана и процедур проверки правильности старта;*
* *руководство по процедуре восстановления.*

Требования к четвертому классу:

*Данные требования полностью совпадают с аналогичными требованиями пятого класса.*

Требования к третьему классу:

*Данные требования полностью совпадают с аналогичными требованиями пятого класса.*

1. Тестовая документация

Требования к пятому классу:

*Должна содержать описание тестов и испытаний, которым подвергался межсетевой экран, и результаты тестирования.*

Требования к четвертому классу:

*Должна содержать описание тестов и испытаний, которым подвергался межсетевой экран, и результаты тестирования.*

Требования к третьему классу:

*Должна содержать описание тестов и испытаний, которым подвергался межсетевой экран, и результаты тестирования.*

1. Конструкторская документация

Требования к пятому классу:

*Должна содержать:*

* *общую схему межсетевого экрана;*
* *общее описание принципов работы межсетевого экрана;*
* *описание правил фильтрации;*
* *описание средств и процесса идентификации и аутентификации;*
* *описание средств и процесса регистрации;*
* *описание средств и процесса контроля над целостностью программной и информационной части межсетевого экрана;*

Требования к четвертому классу:

*Данные требования полностью совпадают с аналогичными требованиями пятого класса по составу документации.*

Требования к третьему классу:

*Данные требования полностью включают аналогичные требования пятого класса по составу документации.*

*Дополнительно документация должна содержать:*

* *описание средств и процесса централизованного управления компонентами межсетевого экрана.*

## 2.5 Виртуальные частные сети (VPN)

В связи с широким распространением Интернет, интранет, экстранет при разработке и применении распределенных информационных сетей и систем одной из самых актуальных задач является решение проблем информационной безопасности.

В последнее десятилетие в связи с бурным развитием Интернет и сетей коллективного доступа в мире произошел качественный скачок в распространении и доступности информации. Пользователи получили дешевые и доступные каналы связи. Стремясь к экономии средств, предприятия используют такие каналы для передачи критичной коммерческой информации. Однако принципы построения Интернет открывают злоумышленникам возможности кражи или преднамеренного искажения информации. Не обеспечена достаточно надежная защита от проникновения нарушителей в корпоративные и ведомственные сети.

Для эффективного противодействия сетевым атакам и обеспечения возможности активного и безопасного использования в бизнесе открытых сетей в начале 90-х годов родилась и активно развивается концепция построения защищенных виртуальных частных сетей - VPN. (Virtual Private Networks).

Концепция построения защищенных виртуальных частных сетей VPN

В основе концепции построения защищенных виртуальных частных сетей VPN лежит достаточно простая идея: если в глобальной сети есть два узла, которые хотят обменяться информацией, то для обеспечения конфиденциальности и целостности передаваемой по открытым сетям информации между ними необходимо построить виртуальный туннель, доступ к которому должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям. Термин «виртуальный» указывает на то, что соединение между двумя узлами сети не является постоянным (жестким) и существует только во время прохождения трафика по сети.

Преимущества, получаемые компанией при формировании таких виртуальных туннелей, заключаются, прежде всего, в значительной экономии финансовых средств.

Функции и компоненты сети VPN

Защищенной виртуальной сетью VPN называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

При подключении корпоративной локальной сети к открытой сети возникают угрозы безопасности двух основных типов:

* несанкционированный доступ к корпоративным данным в процессе их передачи по открытой сети;
* несанкционированный доступ к внутренним ресурсам корпоративной локальной сети, получаемый злоумышленником в результате не санкционированного входа в эту сеть.

Защита информации в процессе передачи по открытым каналам связи основана на выполнении следующих основных функций:

* аутентификации взаимодействующих сторон;
* криптографическом закрытии (шифровании) передаваемых данных;
* проверке подлинности и целостности доставленной информации.

Для этих функций характерна взаимосвязь друг с другом. Их реализация основана на использовании криптографических методов защиты информации.

Для защиты локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды обычно используют межсетевые экраны, поддерживающие безопасность информационного взаимодействия путем фильтрации двустороннего потока сообщений, а также выполнения функций посредничества при обмене информацией. Межсетевой экран располагают на стыке между локальной и открытой сетью. Для защиты отдельного удаленного компьютера, подключенного к открытой сети, программное обеспечение межсетевого экрана устанавливают на этом же компьютере, и такой межсетевой экран называется персональным.

Туннелирование

Защита информации в процессе ее передачи по открытым каналам основана на построении защищенных виртуальных каналов связи, называемых крипто защищенными туннелями. Каждый такой туннель представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографический защищенные пакеты сообщений.

Создание защищенного туннеля выполняют компоненты виртуальной сети, функционирующие на узлах, между которыми формируется туннель. Эти компоненты принято называть инициатором и терминатором туннеля. Инициатор туннеля инкапсулирует (встраивает) пакеты в новый пакет, содержащий наряду с исходными данными новый заголовок с информацией об отправителе и получателе. Хотя все передаваемые по туннелю пакеты являются пакетами IP, инкапсулируемые пакеты могут принадлежать к протоколу любого типа, включая пакеты не маршрутизируемых протоколов, таких, как NetBEUI. Маршрут между инициатором и терминатором туннеля определяет обычная маршрутизируемая сеть IP, которая может быть и сетью отличной от Интернет. Терминатор туннеля выполняет процесс обратный инкапсуляции – он удаляет новые заголовки и направляет каждый исходный пакет в локальный стек протоколов или адресату в локальной сети.

Сама по себе инкапсуляция никак не влияет на защищенность пакетов сообщений, передаваемых по туннелю. Но благодаря инкапсуляции появляется возможность полной криптографической защиты инкапсулируемых пакетов. Конфиденциальность инкапсулируемых пакетов обеспечивается путем их криптографического закрытия, то есть зашифровывания, а целостность и подлинность – путем формирования цифровой подписи. Поскольку существует большое множество методов криптозащиты данных, очень важно, чтобы инициатор и терминатор туннеля использовали одни и те же методы и могли согласовывать друг с другом эту информацию.

Кроме того, для возможности расшифровывания данных и проверки цифровой подписи при приеме инициатор и терминатор туннеля должны поддерживать функции безопасного обмена ключами. Ну и наконец, чтобы туннели создавались только между уполномоченными пользователями, конечные стороны взаимодействия требуется аутентифицировать.

VPN на основе межсетевых экранов

Межсетевые экраны большинства производителей содержат функции туннелирования и шифрования данных. К программному обеспечению собственно межсетевого экрана добавляется модуль шифрования.

В качестве примера решения на базе межсетевых экранов можно назвать FireWall-1 компании Check Point Software Technologies. FairWall-1 использует для построения VPN стандартный подход на базе IPSec. Трафик, приходящий в межсетевой экран, дешифруется, после чего к нему применяются стандартные правила управления доступом. FireWall-1 работает под управлением операционных систем Solaris и Windows NT 4.0.

К недостаткам этого метода относятся высокая стоимость решения в пересчете на одно рабочее место и зависимость производительности от аппаратного обеспечения, на котором работает межсетевой экран. На рис. 2.9 показано пример совмещения межсетевого экрана и VPN.

При использовании межсетевых экранов на базе ПК надо помнить, что подобный вариант подходит только для небольших сетей с ограниченным объемом передаваемой информации.

HTTP - сервер

SMTP - сервер

Рабочие станции

Межсетевой экран и VPN-сервер

Интернет

VPN

Логическое расширение внутренней сети

Незашифрованный трафик

Рис. 2.9. Пример совмещения межсетевого экрана и VPN

# 3. Предложение по совершенствованию защиты компьютерной сети организации за счет внедрение межсетевого экрана

##

## 3.1 Правильный выбор межсетевых экранов для защиты информации КСО

Оптимальные межсетевые экраны для малых и средних организаций с невысокими требованиями к безопасности

В данном разделе, рассматриваются широко распространенные аппаратные межсетевые экраны и приводятся рекомендации по их применению в зависимости от размера организации, требуемого уровня безопасности и стоимости решения. В первой части статьи рассмотрены решения, оптимальные для малых и средних организаций с невысокими требованиями к безопасности, а во второй — решения для малых и средних компаний и офисов филиалов, нуждающихся в надежной защите.

**Выбор варианта**

В настоящее время выбор межсетевых экранов очень широк, начиная от простого (и бесплатного) Windows Firewall, размещаемого на защищаемой машине, до высокопроизводительных межсетевых экранов с проверкой состояния пакетов стоимостью в десятки тысяч долларов. Как выбрать оптимальный вариант для конкретного организация? При выборе межсетевого экрана следует учитывать два основных фактора: требования безопасности и стоимость.

Требования безопасности.

Требования к безопасности постоянно меняются. Администратор должен сочетать надежную защиту с удобством пользовательского доступа к данным, а также учитывать принципиальные ограничения программ, авторы которых обращали мало внимания на безопасность хост-машины и сети.

Ограничения по стоимости. Цена — барьер между желаниями и действительностью. Главное препятствие на пути к высокой безопасности — затраты, которые готов или может нести пользователь. Уровень защиты, обеспечиваемый простым широкополосным маршрутизатором для малого/домашнего офиса с проверкой пакетов, значительно ниже, чем при применении промышленного межсетевого экрана с проверкой пакетов и контролем на прикладном уровне. В целом чем выше стоимость межсетевого экрана, тем надежнее защита. Уровень безопасности соответствует затратам, которые несет организация (на разовое приобретение аппаратных средств и программного обеспечения или на оплату консультантов по управлению недорогими решениями).

Решения, представленные в разделе

Рынок межсетевых экранов чрезвычайно велик и разнообразен, поэтому невозможно оценить каждого поставщика. Чтобы несколько упорядочить картину, было выбрано несколько поставщиков устройств, охватывающих весь спектр надежности и стоимости, от традиционных межсетевых экранов с проверкой пакетов до смешанных устройств с проверкой пакетов и приложений для устранения универсальных угроз (universal threat management, UTM). В данной статье представлены такие поставщики, как Cisco Systems, Network Engines, Rimapp, SonicWall и Symantec.

Главный акцент в обзоре сетевых межсетевых экранов для организаций различных размеров и требований к безопасности сделан на уровне защиты, а не характеристиках маршрутизации или дополнительных функциях устройства. Многие поставщики межсетевых экранов взимают дополнительную плату за передовые функции маршрутизации, которые никак не влияют на уровень безопасности. Например, не рассматривались маршрутизация на базе политик, качество обслуживания, прозрачность уровня управления передачей данных и другие сетевые усовершенствования, которые мало влияют на общую безопасность.

С другой стороны, продукты некоторых поставщиков располагают функциями Web-кэширования, значительно повышающими общую ценность приобретения для организации, которой не приходится покупать отдельное решение для кэширования. В результате повышается производительность при работе в Web и снижаются общие затраты на эксплуатацию канала Internet. Наличие Web-proxy также повышает безопасность.

Характеристики оценки межсетевых экранов

Ниже приводится краткий обзор характеристик, которые принимались во внимание при оценке аппаратных межсетевых экранов. Этот список поможет понять информацию, приведенную в таблице 3.2 и 3.3.

*Цена.* Стоимость конкретных межсетевых экранов у разных продавцов может сильно различаться. Приведенная в данном обзоре цена отражает стандартный набор функций без дополнительных модулей, которые приходится покупать отдельно. Модули расширения могут значительно повысить указанную цену.

*Контроль на прикладном уровне с учетом состояния.* Контроль на прикладном уровне с учетом состояния заключается в проверке как заголовков протокола, так и прикладных данных с использованием механизма контроля на прикладном уровне. Примеры — углубленная проверка на прикладном уровне данных и заголовков HTTP, данных и заголовков SMTP, данных и заголовков протокола Instant Messaging (IM).

*Контроль прикладного протокола.* Контроль прикладного протокола (иначе, углубленная проверка пакетов — deep packet inspection) позволяет анализировать протокол прикладного уровня и подтвердить его соответствие стандартам IETF (Internet Engineering Task Force) для наборов команд протоколов. Примеры — контроль протоколов DNS, FTP, POP3 и SMTP. В процессе контроля прикладного протокола проверка соответствия заданным условиям всех данных на прикладном уровне не выполняется.

*Проверка пакетов на соответствие заданным условиям.* Данный метод обеспечивает проверку заголовков сетевого и транспортного уровня в механизме фильтрации пакетов межсетевого экрана. Проверка пакетов на соответствие заданным условиям применяется практически во всех современных межсетевых экранов и одно время была стандартным методом защиты.

*Прозрачная аутентификация Windows.* Благодаря прозрачной аутентификации межсетевой экран получает учетные данные пользователя из клиентской операционной системы без постороннего вмешательства. Строгий контроль внешнего доступа пользователей и групп осуществляется без запроса учетных данных пользователя.

*Протоколирование всех имен пользователей и приложений Web и Winsock.* Протоколирование — обязательное условие для подготовки исчерпывающих отчетов о соответствии законодательству и эффективного сотрудничества с правоохранительными органами. Через протоколирование имен пользователей и приложений Winsock межсетевой экран получает информацию о приложениях и ресурсах, доступных пользователю при подключении через межсетевой экран.

*Контроль на прикладном уровне через туннели SSL (Secure Sockets Layer).* Такой контроль позволяет выполнить проверку на соответствие заданным условиям и проанализировать протокол соединения в шифрованном туннеле SSL. Межсетевые экраны, которые обеспечивают только проверку пакетов на соответствие заданным условиям, не могут контролировать заголовки и данные прикладного уровня в шифрованных туннелях SSL.

*Поддержка Microsoft Exchange Server.* Межсетевые экраны со встроенной поддержкой Exchange повышают безопасность удаленных соединений через Internet со службами Exchange, в том числе Outlook Web Access (OWA), Outlook Mobile Access (OMA), Exchange ActiveSync, Secure Exchange RPC и RPC over HTTP. Эта характеристика охватывает встроенные функции двухфакторной аутентификации, например RSA SecurID компании RSA Security.

*Контроль шлюзового и клиентского трафика VPN на прикладном уровне.* Благодаря контролю шлюзовых и клиентских соединений VPN межсетевой экран проверяет как пакеты на соответствие заданным условиям, так и туннельные соединения через PPTP, Layer Two Tunneling Protocol (L2TP)/IPsec или IPsec на прикладном уровне. Контроль на прикладном уровне соединений через канал VPN предотвращает распространение таких «червей», как Blaster и Sasser. Например, межсетевой экран ISA Server 2004 компании Microsoft обеспечивает соответствие стандарту вызовов удаленных процедур RPC (remote procedure call) и блокирует Blaster и аналогичные угрозы.

*Обнаружение и предотвращение несанкционированного доступа.* Методы обнаружения и предотвращения несанкционированного доступа ориентированы на аномалии сетевого и транспортного уровня, угрожающие набору протоколов TCP/IP межсетевого экрана. Большинство межсетевых экранов систем обнаружения и предупреждения вторжений Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) можно настроить на пересылку предупреждений администраторам без активных действий или предупреждение с принятием мер для предотвращения нападения. На практике большинство межсетевых экранов IDS/IPS запрещают попытки несанкционированного доступа в момент обнаружения.

*Сервер удаленного доступа VPN и шлюз VPN.* Сервер удаленного доступа VPN принимает клиентские соединения VPN от систем и подключает эту систему в корпоративную сеть. Шлюз VPN связывает целые сети через межсайтовое VPN-соединение.

*VPN-клиент.* Для всех традиционных удаленных клиентских соединений VPN необходима клиентская программа (в бесклиентских SSL VPN в качестве клиента используется браузер). Большинство межсетевых экранов обеспечивают соединения PPTP и L2TP/IPsec со встроенным в Windows VPN-клиентом от Microsoft. Для некоторых межсетевых экранов требуются дополнительная (расширенная) клиентская программа VPN, которая обеспечивает проверку соответствия требованиям безопасности клиента VPN, и специальные протоколы IPsec для прохождения трансляции сетевых адресов NAT (Network Address Translation). Эти программы могут предоставляться бесплатно, но иногда их приходится покупать отдельно.

*10/100-Мбит/с порты локальной сети.* Межсетевой экран с несколькими портами Ethernet, выделенными для локальных соединений, обеспечивает более глубокую физическую сегментацию зон безопасности. В некоторых межсетевых экранов имеется несколько портов Ethernet, но ограничено число портов, которые могут использоваться для подключения к Internet.

*Порты WAN.* В некоторых межсетевых экранов ограничено число портов для прямого подключения к Internet. В других для этой цели можно использовать сколь угодно много портов.

*Балансировка нагрузки.* Несколько межсетевых экранов можно подключить параллельно и балансировать входящие и исходящие соединения через межсетевой экран. В идеальном случае соединения равномерно распределяются между межсетевыми экранами, и результаты работы каждого устройства меняются в лучшую сторону благодаря предотвращению перегрузки отдельных межсетевых экранов.

*Число пользователей.* В некоторых межсетевых экранов ограничено число пользователей или IP-адресов, которые могут устанавливать соединения через межсетевой экран. Эти межсетевые экраны лицензированы для работы с определенным числом пользователей и, если превышен лицензионный порог, генерируют соответствующее предупреждение.

*Передача функций отказавшего межсетевого экрана исправному устройству.* Данная функция позволяет подключить два или несколько межсетевых экранов таким образом, чтобы они могли обслуживать соединения вместо отказавших устройств. Резервирование может быть «холодным» (без нагрузки), «горячим» (под нагрузкой) или с балансировкой нагрузки. Некоторые процедуры переключения автоматические, а в других случаях требуется вмешательство администратора.

*Переключение Internet-провайдера и объединение полосы пропускания.*Возможность работы с несколькими Internet-провайдерами — важнейшее требование любой организации, деятельность которой зависит от связи с Internet. Межсетевые экраны со сменой Internet-провайдеров могут переключаться на работоспособную линию, если связь с одним или несколькими провайдерами прерывается. Объединение полосы пропускания заключается в соединении нескольких линий связи в скоростной канал доступа к ресурсам Internet.

*Настройка.* Большинство межсетевых экранов обеспечивают Web-соединения SSL в некоторых или во всех конфигурациях. Некоторые межсетевые экраны поддерживают интерфейс командной строки в сеансе терминала, а межсетевые экраны на базе ISA Server обеспечивают шифрованные соединения RDP, совместимые со стандартом обработки информации FIPS (Federal Information Processing Standard).

*Процессор.* Данная характеристика в пояснениях не нуждается. Она указывает тип и быстродействие основного процессора межсетевого экрана.

*Web-кэширование и proxy-сервер.* Некоторые межсетевые экраны располагают встроенным сервером Web-кэширования. Web-кэширование ускоряет доступ в Internet для конечных пользователей и может существенно понизить нагрузку на канал связи с Internet и соответствующие расходы. Компонент Web-proxy значительно повышает безопасность, полностью разлагая на составные части, а затем проверяя и восстанавливая проходящие через него сообщения HTTP.

Низкий уровень безопасности

Как отмечалось в начале статьи, межсетевые экраны рассматриваются в соответствии с необходимым предприятию уровнем безопасности. Межсетевые экраны первого типа предназначены для малых и средних предприятий с низким уровнем безопасности. В слабо защищенной среде важные данные не хранятся в сети или владелец конфиденциальной информации не может либо не хочет платить за сетевой межсетевой экран с мощными функциями проверки входящего и исходящего доступа, пакетов и прикладного уровня, исчерпывающее протоколирование действий пользователей и приложений.

Как правило, слабо защищенные сети принадлежат небольшим компаниям с ограниченным бюджетом. Локальная сеть может подключаться к Internet через широкополосный кабельный модем или DSL-соединение с помощью так называемого «широкополосного маршрутизатора» вместо выделенных линий уровней T и выше, более распространенных в крупных организациях. Технически широкополосные маршрутизаторы не относятся к маршрутизаторам, а представляют собой простые устройства NAT. Большинство таких устройств позволяет установить немногочисленные VPN-соединения с использованием фирменных клиентских программ VPN.

Верхняя граница ценового диапазона межсетевых экранов для среды с невысоким уровнем защиты — около 500 долл. Если на сеть с низким уровнем безопасности не распространяются строгие требования правоохранительного надзора, а компания имеет очень ограниченный бюджет, то следует обратить внимание на продукты Cisco, SonicWall и Symantec, сравнительные характеристики которых приведены в таблице 3.1.

Три межсетевого экрана располагают сходной функциональностью, возможностями и уровнями защиты от внешних угроз. Каждый обеспечивает проверку пакетов на соответствие заданным условиям во входящих соединениях с Internet. Этим маломощным устройствам свойственны существенные ограничения по числу пользователей. Число соединений определяется схемой лицензирования каждого поставщика и возможностями аппаратных средств.

Еще важнее, что эти межсетевые экраны не располагают средствами контроля входящего и исходящего доступа по пользователям и группам. Функции протоколирования всех устройств примитивны. Отсутствует проверка на соответствие заданным условиям на прикладном уровне. Эти ограничения типичны для недорогих аппаратных межсетевых экранов.

Из этой тройки рекомендуется использовать простое в настройке устройство SonicWall 170, которое работает почти автоматически. SonicWall 170 располагает модемным интерфейсом, благодаря которому возможно переключение на аналоговое модемное соединение в случае отказа основного широкополосного канала связи. Кроме того, в SonicWall 170 на один локальный порт больше, чем в двух других устройствах.

Сетевая безопасность — решающий компонент общей стратегии эшелонированной обороны предприятия. Сетевые межсетевые экраны — ключевые элементы защиты систем и данных на различных сетевых периметрах. Предприятия с низкими требованиями к безопасности могут выбрать один из межсетевых экранов из таблицы или другие продукты такого уровня, но для надежной защиты требуются устройства, которые будут рассмотрены чуть ниже.

Таблица 3.1. Аппаратные межсетевые экраны для сетевой среды с невысокой надежностью

|  |  |  |  |
| --- | --- | --- | --- |
|  | SonicWall 170 | Cisco PIX 501 | Symantec Firewall/VPN |
| Цена в долларах | 410 | 495 | 499 |
| Контроль на прикладном уровне с учетом состояния | Нет | Нет | Нет |
| Контроль прикладного протокола | Да (ограничено) | Да (ограничено) | Да (ограничено) |
| Проверка пакетов на соответствие заданным условиям | Да | Да | Да |
| Прозрачная аутентификация Windows | Нет | Нет | Нет |
| Протоколирование всех имен пользователей и приложений Web и Winsock | Нет | Нет | Нет |
| Контроль на прикладном уровне через туннели SSL | Нет | Нет | Нет |
| Поддержка Exchange | Нет | Нет | Нет |
| Контроль шлюзового и клиентского трафика VPN на прикладном уровне | Нет | Нет | Нет |
| Обнаружение и предотвращение несанкционированного доступа | Да | Да | Да |
| Сервер удаленного доступа VPN и шлюз VPN | Да | Да | Нет |
| VPN-клиент | Нет | Нет | Нет |
| 10/100-Мбит/с порты ЛВС | 5 | 4 | 4 |
| Порты WAN | 1 | 1 | 1 |
| Балансировка нагрузки | Нет | Нет | Нет |
| Число пользователей | 10 | 10 | 15-25 |
| Передача функций отказавшего межсетевого экрана исправному устройству | Аналоговый коммутируемый доступ через внешний модем | Нет | Аналоговый коммутируемый доступ через внешний модем |
| Переключение Internet-провайдера и объединение полосы пропускания | Нет | Нет | Нет |
| Настройка | Web-интерфейс | Командная строка и Web-интерфейс | Web-интерфейс |
| Процессор | SonicWall Security Processor | AMD SC520 | ARM7 |
| Web-кэширование и proxy-сервер | Нет | Нет | Нет |

Варианты для малых и средних предприятий с высокими требованиями к безопасности

В тех организациях, где защите приходится уделять много внимания, к межсетевым экранам предъявляются гораздо более высокие требования. Повышенная безопасность может быть вызвана условиями закона, характером бизнеса (например, в отраслях с острой конкуренцией необходимо охранять коммерческие секреты) или желанием владельца получить достойную защиту по разумной цене. В малых и средних компаниях с высокими требованиями к безопасности к межсетевому экрану относятся, как к страхованию автомобиля. Такие организации готовы заплатить вперед, чтобы предотвратить потенциальную катастрофу.

Проблемы обеспечения высокого уровня безопасности

При выборе межсетевого экрана с повышенным уровнем защиты необходимо учитывать ряд дополнительных требований.

* Следует протоколировать обращения из корпоративной сети в Internet. Как минимум, требуется записывать имя пользователя и приложение, задействованное при попытках получить доступ к ресурсам через межсетевой экран. Рекомендуется также указывать имена сайтов и тип контента.
* Необходим механизм настройки межсетевого экрана на блокирование запуска приложений, которые представляют опасность для сети и целостности данных - например, одноранговых (P2P) сетей и программ мгновенного обмена сообщениями (Instant Messaging - IM).
* Межсетевой экран должен останавливать как входящий, так и исходящий несанкционированный трафик, с проверкой пакетов на соответствие заданным условиям и контролем на прикладном уровне по всем интерфейсам, в том числе VPN.
* Межсетевой экран должен обеспечивать проверку пакетов на соответствие заданным условиям и контроль на прикладном уровне для входящего трафика, проходящего через межсетевой экран в корпоративную сеть, чтобы удаленные пользователи могли обращаться к данным предприятия извне. Проверка на соответствие заданным условиям должна производиться над данными, зашифрованными для передачи по линиям связи.
* Блокировать или смягчать действие червей, вирусов, шпионских программ и других угроз для целостности данных на периметре сети; контроль на прикладном уровне необходим на всех этапах.
* Если требуется доступ к важной бизнес - информации, следует предусмотреть механизмы обеспечения отказоустойчивости.

Несмотря на высокие требования к безопасности, предъявляемые некоторыми малыми предприятиями, эти компании все же остаются малыми и не располагают бюджетом крупных корпораций. В среднем малая организация готова потратить до 3000 долл. на решение для обеспечения безопасности, срок эксплуатации которого составит 3-4 года. Ежедневная цена решения с учетом амортизации (около 2 долл. в день) невелика по сравнению с потенциальными финансовыми потерями, которые могут стать следствием выбора ненадежного решения.

**Выбор устройств**

В таблице 3.2 приведены аппаратные межсетевые экраны, которые обеспечивают приемлемую сетевую безопасность для нуждающихся в серьезной защите малых и средних предприятий. SonicWALL Pro 3060 и Cisco PIX-515E-RDMZ компании Cisco Systems — традиционные аппаратные межсетевые экраны. NS6200 компании Network Engines на базе Microsoft ISA Server 2004 и SGS 5420 компании Symantec представляют собой продукты, которые обычно называют «программными» межсетевыми экранами — они работают на базе универсальной операционной системы или имеют жесткие диски (иногда присутствуют оба компонента). NS6200 относится к «третьему поколению» межсетевых экранов, в котором стабильность и надежность аппаратного межсетевого экрана сочетаются с гибкостью, удобством обновления и готовностью отразить новейшие угрозы программного продукта. Характеристики SGS 5420 — промежуточные: он не работает с универсальной операционной системой, но располагает жестким диском.

Для безопасности сети рекомендуется устройства Network Engines и Symantec, которые превосходят традиционные аппаратные модели с проверкой пакетов на соответствие заданным условиям. Главное различие заключается в глубине контроля на прикладном уровне, обеспечиваемом этими двумя устройствами, по сравнению с межсетевыми экранами SonicWALL и Cisco.

Для контроля на прикладном уровне в межсетевых экранов этого класса можно использовать встраиваемые и внешние модули расширения (например, для борьбы с вирусами, фильтрации загружаемых файлов, фильтрации почты, блокирования всплывающей рекламы, анализа Web-контента). При этом из-за высокой цены устройства могут оказаться недосягаемыми для малых и средних предприятий.

В конечном итоге было отдано межсетевому экрану Network Engines предпочтение перед устройством Symantec благодаря достоинствам, решающим для создания сетевой среды с высоким уровнем безопасности.

* Прозрачная аутентификация всех исходящих соединений через межсетевой экран. В среде с высоким уровнем безопасности для регистрации в домене требуется двухфакторная аутентификация. Благодаря прозрачной аутентификации, пользователи не могут обмениваться учетными данными для доступа к Internet, так как система никогда не выводит на экран окно регистрации. В результате повышаются достоверность данных в журнале и эффективность дальнейшего расследования на основе этой информации.
* Полное протоколирование всех входящих и исходящих соединений через межсетевой экран. Эти сведения, в том числе об именах пользователей и приложениях, задействованных для доступа к любым ресурсам через межсетевой экран, незаменимы при выполнении аудита на соответствие законодательству и в ходе административных, уголовных и гражданских расследований.
* Контроль на прикладном уровне туннелей SSL (Secure Sockets Layer - уровень защищенных гнезд). Устройство NS6200 на базе ISA Server 2004 выполняет контроль на прикладном уровне входящих соединений SSL через межсетевой экран. Такие соединения могут использоваться для обращений к частным данным на сервере Microsoft Outlook Web Access (OWA) или Microsoft SharePoint Portal Server. В отличие от других межсетевых экранов в таблице 3.2, NS6200 может дешифровать SSL-соединение в межсетевом экране, передать заголовки и данные в механизм прикладного управления межсетевого экрана, а затем заново зашифровать данные для сквозной пересылки по безопасному шифрованному соединению.
* Проверка пакетов на соответствие заданным условиям и контроль на прикладном уровне по всем VPN-интерфейсам. Данная проверка охватывает VPN удаленного доступа и шлюзовые соединения между сайтами. Каналы VPN нередко оказываются слабым звеном во многих межсетевых экранов, так как подключенные к VPN машины, как правило, рассматриваются как "доверенные" и не подвергаются контролю на прикладном уровне. Такой подход был главной причиной атаки червя Blaster на сети, в остальном защищенные от внешней угрозы. Опасности, аналогичные Blaster, все еще существуют, и VPN-соединения по-прежнему могут служить средой их распространения. NS6200 открывает каналы VPN для контроля на прикладном уровне и блокирует нападения на межсетевом экране.

Даже вместе с дорогостоящими модулями расширения для контроля на прикладном уровне ни один из остальных межсетевых экранов в табл. 3.2 не располагает функциями безопасности, реализованными в NS6200.

Более масштабные сети с высоким уровнем защиты

Средним и крупным предприятиям, а также их филиалам свойственны похожие требования к безопасности. Как и небольшим компаниям с надежной защитой, им требуются исчерпывающая проверка пакетов на соответствие заданным условиям и контроль на прикладном уровне, полное протоколирование и функции управления доступом пользователей/групп через межсетевой экран. Основное различие между надежно защищенной крупной компанией и малым предприятием заключается в гораздо больших финансовых возможностях корпорации, которые соответствуют требованиям информационной безопасности.

Таким фирмам не нужны самые технологичные и производительные межсетевые экраны стоимостью 35 тыс. долл., им скорее требуется надежная информационная защита. Единственная атака на прикладном уровне может привести к потерям, исчисляемым миллионами долларов.

Выяснить, сколько денег организации этого типа готовы потратить на защиту межсетевым экраном, нелегко. Некоторые компании придают безопасности чрезвычайно большое значение и готовы заплатить более 10 тыс. долл. за превосходный межсетевой экран с проверкой пакетов и контролем на прикладном уровне. С другой стороны, многие средние и крупные предприятия, которые нуждаются в надежной защите, неохотно платят более 2500 долл. за этот решающий компонент инфраструктуры сетевой безопасности. В целом большинство организаций такого размера охотно тратит от 5000 до 6000 долл. за хороший межсетевой экран.

В таблице 3.3 показан выбор межсетевых экранов, обычно развертываемых в более крупных предприятиях с высоким уровнем безопасности. SonicWALL PRO 4060 и Cisco PIX 515E-UR-FE-BUN выполнены на основе традиционного аппаратного межсетевого экрана и обеспечивают соответствующий уровень сетевой безопасности. Проверка пакетов на соответствие заданным условиям — основа этих продуктов обеспечения безопасности, для ее реализации не требуется дорогостоящих модулей расширения. Обе модели отличаются высокой производительностью, но им не хватает возможностей балансировки нагрузки и передачи функций отказавшего устройства исправному, если они крайне необходимы для бесперебойного доступа к важнейшим данным.

В отличие от них, устройство RoadBLOCK F302PLUS на базе ISA Server 2004 компании RimApp обеспечивает исчерпывающий контроль на прикладном уровне по приемлемой цене. В стандартной конфигурации реализованы фильтры Web-узлов, проверка загружаемых из Internet файлов на вирусы и фильтры спама. Кроме того, с помощью модулей RainWall и RainConnect компании Rainfinity устройство RoadBLOCK обеспечивает балансировку нагрузки и передачу функций отказавшего устройства исправному как для аппаратных межсетевых экранов RoadBLOCK, так и для каналов связи Internet-провайдеров. Устройство RoadBLOCK поддерживает все упомянутые выше высокоуровневые функции подготовки отчетов и протоколирования и располагает мощными функциями управления пользовательским и групповым доступом из входящих и исходящих соединений через межсетевой экран.

Оптимальный выбор

Высокоуровневые сетевые межсетевые экраны, представленные в данном разделе, обеспечивают превосходный уровень безопасности и высокую производительность для средних и крупных предприятий. При выборе оптимального межсетевого экрана следует в первую очередь обратить внимание на контроль на прикладном уровне и исчерпывающие возможности протоколирования и подготовки отчетов о доступе пользователей и приложений. Кроме того, при выборе аппаратного межсетевого экрана важно помнить об отказоустойчивости.

Таблица 3.2. Аппаратные межсетевые экраны для малых предприятий с высокими требованиями к безопасности

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Характеристика | SonicWALL Pro 3060 | Cisco PIX-515E-R-DMZ | Network Engines NS6200 | Symantec SGS 5420 |
| Цена в долларах | 2319 | 2699 | 2499 | 2999 |
| Контроль на прикладном уровне с учетом состояния | Нет | Да (ограничено) | Да (умеренно) | Да (ограничено) |
| Контроль прикладного протокола | Да | Да | Да | Да |
| Проверка пакетов на соответствие заданным условиям | Да | Да | Да | Да |
| Прозрачная аутентификация Windows | Нет | Нет | Да | Нет |
| Протоколирование всех имен пользователей и приложений Web и Winsock | Нет | Нет | Да | Нет |
| Контроль на прикладном уровне через туннели SSL | Нет | Нет | Да | Нет |
| Поддержка Exchange | Нет | Нет | Да | Нет |
| Контроль шлюзового и клиентского трафика VPN на прикладном уровне | Нет | Нет | Да | Нет |
| Обнаружение и предотвращение несанкционированного доступа | Да | Да | Да | Да |
| Сервер удаленного доступа VPN и шлюз VPN | Да | Да | Да | Да |
| VPN-клиент | Нет | Да | Да | Нет |
| 10/100-Мбит/с порты ЛВС | 5 | 2 | 3 | 5 |
| Порты WAN | 1 | 1 | 1 | 1 |
| Балансировка нагрузки | Нет | Нет | Да | Нет |
| Число пользователей | Неогр. | Неогр. | Неогр. | 50 |
| Передача функций отказавшего межсетевого экрана исправному устройству | Нет | Нет | Нет | Нет |
| Переключение Internet-провайдера и полосы пропускания | Нет | Нет | Нет |   |
| Настройка | Web-интерфейс | Командная строка и Web-интерфейс | Ограниченный Web и FIPS-совместимый RDP | Web-интерфейс |
| Процессор | 2-ГГц Intel | 1-ГГц Intel | 2-ГГц Intel | Intel |
| Web-кэширование и proxy | Нет | Нет | Да | Нет |

Таблица 3.3. Аппаратные межсетевые экраны для крупных предприятий с высокими требованиями к безопасности

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристика | SonicWALL Pro 4060 | Cisco PIX-515E UR-FE-BUN | RimApp RoadBLOCK F302PLUS |
| Цена в долларах | 4995 | 5145 | 5580 |
| Контроль на прикладном уровне с учетом состояния | Нет | Да (ограничено) | Да |
| Контроль прикладного протокола | Да | Да | Да |
| Проверка пакетов на соответствие заданным условиям | Да | Да | Да |
| Прозрачная аутентификация Windows | Нет | Нет | Да |
| Протоколирование всех имен пользователей и приложений Web и Winsock | Нет | Нет | Да |
| Контроль на прикладном уровне через туннели SSL | Нет | Нет | Да |
| Поддержка Exchange | Нет | Нет | Да |
| Контроль шлюзового и клиентского трафика VPN на прикладном уровне | Нет | Нет | Да |
| Обнаружение и предотвращение несанкционированного доступа | Да | Да | Да |
| Сервер удаленного доступа VPN и шлюз VPN | Да | Да | Да |
| VPN-клиент | Нет | Да | Да |
| 10/100-Мбит/с порты ЛВС | 5 | 6 | 2-5 |
| Порты WAN | 1 | 1-4 | 1-5 |
| Балансировка нагрузки | Нет | Нет | Да |
| Число пользователей | Неограниченно | Неограниченно | Неограниченно |
| Передача функций отказавшего межсетевого экрана исправному устройству | Да | Да | Да |
| Переключение Internet-провайдера и объединение полосы пропускания | Да | Нет | Да |
| Конфигурирование Web-интерфейс | Командная строка и Web-интерфейс | Исчерпывающий Web и FIPS-совместимый RDP |   |
| Процессор | 2-ГГц Intel | 433-МГц Celeron | 2,8-ГГц Intel |
| Web - кэширование и proxy | Нет | Нет | Да |

## 3.2 Intrusion Detection Systems (IDS)

Система обнаружение вторжение

IDS являются программными или аппаратными системами, которые автоматизируют процесс просмотра событий, возникающих в компьютерной системе или сети, и анализируют их с точки зрения безопасности. Так как количество сетевых атак возрастает, IDS становятся необходимым дополнением инфраструктуры безопасности.

Обнаружение проникновения является процессом мониторинга событий, происходящих в компьютерной системе или сети, и анализа их. Проникновения определяются как попытки компрометации конфиденциальности, целостности, доступности или обхода механизмов безопасности компьютера или сети. Проникновения могут осуществляться как атакующими, получающими доступ к системам из Интернета, так и авторизованными пользователями систем, пытающимися получить дополнительные привилегии, которых у них нет. IDS являются программными или аппаратными устройствами, которые автоматизируют процесс мониторинга и анализа событий, происходящих в сети или системе, с целью обнаружения проникновений.

IDS состоят из трех функциональных компонентов: информационных источников, анализа и ответа. Система получает информацию о событии из одного или более источников информации, выполняет определяемый конфигурацией анализ данных события и затем создает специальные ответы – от простейших отчетов до активного вмешательства при определении проникновений.

Почему следует использовать IDS

Обнаружение проникновения позволяет организациям защищать свои системы от угроз, которые связаны с возрастанием сетевой активности и важностью информационных систем. При понимании уровня и природы современных угроз сетевой безопасности, вопрос не в том, следует ли использовать системы обнаружения проникновений, а в том, какие возможности и особенности систем обнаружения проникновений следует использовать.

Почему следует использовать IDS, особенно если уже имеются межсетевые экраны, антивирусные инструментальные средства и другие средства защиты?

Каждое средство защиты адресовано конкретной угрозе безопасности в системе. Более того, каждое средство защиты имеет слабые и сильные стороны. Только комбинируя их (данная комбинация иногда называет безопасностью в глубину), можно защититься от максимально большого спектра атак.

Межсетевые экраны являются механизмами создания барьера, преграждая вход некоторым типам сетевого трафика и разрешая другие типы трафика. Создание такого барьера происходит на основе политики межсетевого экрана. IDS служат механизмами мониторинга, наблюдения активности и принятия решений о том, являются ли наблюдаемые события подозрительными. Они могут обнаружить атакующих, которые обошли межсетевой экран, и выдать отчет об этом администратору, который, в свою очередь, предпримет шаги по предотвращению атаки.

IDS становятся необходимым дополнением инфраструктуры безопасности в каждой организации. Технологии обнаружения проникновений не делают систему абсолютно безопасной. Тем не менее практическая польза от IDS существует, и не маленькая. Использование IDS помогает достичь нескольких целей:

1. Возможность иметь реакцию на атаку позволяет заставить атакующего нести ответственность за собственную деятельность. Это определяется следующим образом: "Я могу прореагировать на атаку, которая произведена на мою систему, так как я знаю, кто это сделал или где его найти". Это трудно реализовать в сетях TCP/IP, где протоколы позволяют атакующим подделать идентификацию адресов источника или другие идентификаторы источника. Также очень трудно осуществить подотчетность в любой системе, которая имеет слабые механизмы идентификации и аутентификации.
2. Возможность блокирования означает возможность распознать некоторую активность или событие как атаку и затем выполнить действие по блокированию источника. Данная цель определяется следующим образом: "Я не забочусь о том, кто атакует мою систему, потому что я могу распознать, что атака имеет место, и блокировать ее". Заметим, что требования реакции на атаку полностью отличаются от возможности блокирования.

Атакующие, используя свободно доступные технологии, могут получить неавторизованный доступ к системам, если найденные в системах уязвимости не исправлены, а сами системы подсоединены к публичным сетям.

Объявления о появлении новых уязвимостей являются общедоступными, например, через публичные сервисы, такие как ICAT или CERT, которые созданы для того, чтобы эти уязвимости нельзя было использовать для выполнения атак. Тем не менее, существует много ситуаций, в которых использование этих уязвимостей все же возможно:

* Во многих наследуемых системах не могут быть выполнены все необходимые обновления и модификации.
* Даже в системах, в которых обновления могут быть выполнены, администраторы иногда не имеют достаточно времени или ресурсов для отслеживания и инсталлирования всех необходимых обновлений. Это является общей проблемой, особенно в окружениях, включающих большое количество хостов или широкий спектр аппаратуры и ПО.
* Пользователям могут требоваться функциональности сетевых сервисов и протоколов, которые имеют известные уязвимости.
* Как пользователи, так и администраторы делают ошибки при конфигурировании и использовании систем.
* При конфигурировании системных механизмов управления доступом для реализации конкретной политики всегда могут существовать определенные несоответствия. Такие несоответствия позволяют законным пользователям выполнять действия, которые могут нанести вред или которые превышают их полномочия.

В идеальном случае производители ПО должны минимизировать уязвимости в своих продуктах, и администраторы должны быстро и правильно корректировать все найденные уязвимости. Однако в реальной жизни это происходит редко, к тому же новые ошибки и уязвимости обнаруживаются ежедневно.

Поэтому обнаружение проникновения может являться отличным выходом из существующего положения, при котором обеспечивается дополнительный уровень защиты системы. IDS может определить, когда атакующий осуществил проникновение в систему, используя нескорректированную или некорректируемую ошибку. Более того, IDS может служить важным звеном в защите системы, указывая администратору, что система была атакована, чтобы тот мог ликвидировать нанесенный ущерб. Это гораздо удобнее и действеннее простого игнорирования угроз сетевой безопасности, которое позволяет атакующему иметь продолжительный доступ к системе и хранящейся в ней информации.

1. Возможно определение преамбул атак, обычно имеющих вид сетевого зондирования или некоторого другого тестирования для обнаружения уязвимостей, и предотвращения их дальнейшего развития.

Когда нарушитель атакует систему, он обычно выполняет некоторые предварительные действия. Первой стадией атаки обычно является зондирование или проверка системы или сети на возможные точки входа. В системах без IDS атакующий свободно может тщательно анализировать систему с минимальным риском обнаружения и наказания. Имея такой неограниченный доступ, атакующий в конечном счете может найти уязвимость и использовать ее для получения необходимой информации.

Та же самая сеть с IDS, просматривающей выполняемые операции, представляет для атакующего более трудную проблему. Хотя атакующий и может сканировать сеть на уязвимости, IDS обнаружит сканирование, идентифицирует его как подозрительное, может выполнить блокирование доступа атакующего к целевой системе и оповестит персонал, который в свою очередь может выполнить соответствующие действия для блокирования доступа атакующего. Даже наличие простой реакции на зондирование сети будет означать повышенный уровень риска для атакующего и может препятствовать его дальнейшим попыткам проникновения в сеть.

1. Выполнение документирования существующих угроз для сети и систем.

При составлении отчета о бюджете на сетевую безопасность бывает полезно иметь документированную информацию об атаках. Более того, понимание частоты и характера атак позволяет принять адекватные меры безопасности.

1. Обеспечение контроля качества разработки и администрирования безопасности, особенно в больших и сложных сетях и системах.

Когда IDS функционирует в течении некоторого периода времени, становятся очевидными типичные способы использования системы. Это может выявить изъяны в том, как осуществляется управление безопасностью, и скорректировать это управление до того, как недостатки управления приведут к инцидентам.

1. Получение полезной информации о проникновениях, которые имели место, с предоставлением улучшенной диагностики для восстановления и корректирования вызвавших проникновение факторов.

Даже когда IDS не имеет возможности блокировать атаку, она может собрать детальную, достоверную информацию об атаке. Данная информация может лежать в основе соответствующих законодательных мер. В конечном счете, такая информация может определить проблемы, касающиеся конфигурации или политики безопасности.

1. IDS помогает определить расположение источника атак по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

Типы IDS

Существует несколько способов классификации IDS, каждый из которых основан на различных характеристиках IDS. Тип IDS следует определять, исходя из следующих характеристик:

*Способ мониторинга системы.* По способам мониторинга системы делятся на network-based, host-based и application-based.

*Способ анализа.* Это часть системы определения проникновения, которая анализирует события, полученные из источника информации, и принимает решения, что происходит проникновение. Способами анализа являются обнаружение злоупотреблений (misuse detection) и обнаружение аномалий (anomaly detection).

*Задержка во времени* между получением информации из источника и ее анализом и принятием решения. В зависимости от задержки во времени, IDS делятся на interval-based (или пакетный режим) и real-time.

Большинство коммерческих IDS являются real-time network-based системами.

К характеристикам IDS также относятся:

*Источник информации.* IDS может использовать различные источники информации о событии для определения того, что проникновение произошло. Эти источники могут быть получены из различных уровней системы, из сети, хоста и приложения.

*Ответ:* Набор действий, которые выполняет система после определения проникновений. Они обычно разделяются на активные и пассивные меры, при этом под активными мерами понимается автоматическое вмешательство в некоторую другую систему, под пассивными мерами — отчет IDS, сделанный для людей, которые затем выполнят некоторое действие на основе данного отчета.

Развертывание IDS

Технология обнаружения проникновений является необходимым дополнением для инфраструктуры сетевой безопасности в каждой большой организации. Эффективное развертывание IDS требует тщательного планирования, подготовки, прототипирования, тестирования и специального обучения.

Следует тщательно выбирать стратегию обнаружения проникновения, совместимую с сетевой инфраструктурой, политикой безопасности и имеющимися ресурсами.

Стратегия развертывания IDS

Следует определить несколько стадий развертывания IDS, чтобы персонал мог получить опыт и создать необходимый мониторинг и необходимое количество ресурсов для функционирования IDS. Требуемые ресурсы для каждого типа IDS могут сильно различаться, в частности, и в зависимости от системного окружения. Необходимо иметь соответствующую политику безопасности, планы и процедуры, чтобы персонал знал, как обрабатывать различные многочисленные сигналы тревоги, выдаваемые IDS.

Для защиты сети предприятия рекомендуется рассмотреть комбинацию network-based IDS и host-based IDS. Далее следует определить стадии развертывания, начиная с network-based IDS, так как они обычно являются более простыми для инсталлирования и сопровождения. После этого следует защитить критичные серверы с помощью host-based IDS. Используя инструментальные средства анализа уязвимостей, следует протестировать IDS и другие механизмы безопасности относительно правильного конфигурирования и функционирования.

Такие технологии, как Honey Pot и аналогичные, должны использоваться только в том случае, если имеется достаточная техническая квалификация администратора. Более того, эти технологии должны использоваться только после анализа существующего законодательства.

Развертывание network-based IDS

Единственный вопрос, который следует тщательно продумать при развертывании network-based IDS, — это расположение системных сенсоров. Существует много вариантов расположения network-based IDS, каждый из которых имеет свои преимущества:

1. Основная подсеть
2. Подсеть с критичными ресурсами и дополнительными точками доступа
3. DMZ-сеть

Рис. 3.1. Возможные варианты расположения сенсоров network-based IDS

*Позади внешнего межсетевого экрана в DMZ-сети (расположение 1)*

Преимущества:

* Видит атаки, исходящие из внешнего мира, которым удалось преодолеть первую линию обороны сетевого периметра.
* Может анализировать проблемы, которые связаны с политикой или производительностью межсетевого экрана, обеспечивающего первую линию обороны.
* Видит атаки, целями которых являются прикладные серверы (такие как web или ftp), обычно расположенные в DMZ.
* Даже если входящая атака не распознана, IDS иногда может распознать исходящий трафик, который возникает в результате компрометации сервера.

*Перед внешним межсетевым экраном (расположение 2)*

Преимущества:

* Документирует количество атак, исходящих из Интернета, целью которых является сеть.
* Документирует типы атак, исходящих из Интернета, целью которых является сеть.

*На основной магистральной сети (расположение 3)*

Преимущества:

* Просматривает основной сетевой трафик; тем самым увеличивается вероятность распознания атак.
* Определяет неавторизованную деятельность авторизованных пользователей внутри периметра безопасности организации.

*В критичных подсетях (расположение 4)*

Преимущества:

* Определяет атаки, целью которых являются критичные системы и ресурсы.
* Позволяет фокусироваться на ограниченных ресурсах наиболее значимых информационных ценностей, расположенных в сети.

Развертывание host-based IDS

После того как network-based IDS размещены и функционируют, для увеличения уровня защиты системы дополнительно может быть рассмотрено использование host-based IDS. Однако инсталлирование host-based IDS на каждый хост может потребовать существенных временных затрат. Поэтому рекомендуется, чтобы в первую очередь host-based IDS были инсталлированы на критичных серверах. Это может уменьшить общую стоимость развертывания и позволит основное внимание уделить реагированию на тревоги, касающиеся наиболее важных хостов. После того как host-based IDS начали функционировать в обычном режиме, организации с повышенными требованиями к безопасности могут обсудить возможность инсталлирования host-based IDS на другие хосты. В этом случае следует приобретать host-based системы, которые имеют централизованное управление и функции создания отчетов. Такие возможности могут существенно понизить сложность управления сообщениями о тревогах от большого числа хостов.

Далее следует рассмотреть возможность повышения квалификации администраторов. В большинстве случаев эффективность конкретной host-based IDS зависит от возможности администратора различать ложные и верные тревоги.

Также важно (так как часто администратор не сопровождает постоянно host-based IDS) установить график проверки результатов IDS. Если это не сделано, риск, что противник изменит что-либо в IDS в течение осуществления атаки, возрастает.

Стратегии оповещения о тревогах

Наконец, при развертывании IDS важной проблемой является определение того, какие именно возможности оповещения IDS о тревогах использовать в каждом конкретном случае. Большинство IDS поставляются с уже сконфигурированными возможностями оповещения о тревогах, которые допускают широкий диапазон опций, включая посылку сообщений на e-mail, пейджер, использование протоколов сетевого управления и даже автоматическое блокирование источника атаки.

Важно быть консервативным в использовании этих возможностей до тех пор, пока не будет стабильной инсталляции IDS и некоторого понимания поведения IDS в данном окружении. Иногда рекомендуется не активизировать оповещения о тревогах IDS в течение нескольких месяцев после инсталляции.

## 3.3 IPv6 как сильное влияние на конструкцию межсетевого экрана

Из всех новшеств, которые появились в ближайшие несколько лет, самое сильное влияние на конструкцию межсетевых экранов окажет одно - новое поколение протокола IP.

Текущей, четвертой версии протокола IP (или IPv4) уже почти 20 лет, и ее возраст начинает сказываться. Адресное пространство IPv4 быстро исчерпывается. Хакеры постоянно находят новые способы эксплуатации слабостей протокола и основанных на нем служб. Новые службы могли бы быть более надежными, если бы таким был сам протокол, лежащий в основе Интернет. Очевидно, что по всем этим и другим причинам в ближайшем будущем произойдет переход на новую, шестую версию протокола IP (IPv6). Работа над IPv6 началась в начале 90-х, а первый предложенный стандарт был одобрен в ноябре 1994 года в документе RFC 1752 «The Recommendation for the IP Next Generation Protocol».

IPv6 сможет взаимодействовать с IPv4, и скорее всего развертывание IPv6 произойдет путем плавной замены, в процессе которой оба протокола будут мирно сосуществовать.

Совместная работа IPv4 и IPv6

Как будет обеспечиваться возможность совместной работы IPv4 и IPv6 в одной сети? В настоящий момент для этого предлагается два метода. Первый из них состоит в использовании в системах с IPv6 двух различных стеков протоколов, одного для IPv4, а другого для IPv6. Их выбор будет определяться типом протокола, применяемого на узле, с которым устанавливается соединение. Второй метод заключается в туннелировании пакетов IPv6 внутри пакетов IPv4 при обмене данными между компьютерами с IPv6 по маршруту, содержащему компьютеры с IPv4.

Заголовок IPv6

Длина нового заголовка IP-пакета равна 40 байтам. Благодаря тому, что эта величина фиксирована, сетевые устройства смогут обрабатывать пакеты намного быстрее. На рис. 3.2 видно, что новый заголовок содержит меньше полей, чем заголовок IPv4.

Кроме уменьшения количества полей, самым заметным отличием заголовка IPv6 является больший размер полей адреса. Поля отправителя и получателя имеют 128 бит, что позволит создать достаточное количество адресов для уникальной идентификации каждой песчинки на планете. Этого должно хватить, по крайней мере, еще на несколько лет.

|  |  |  |
| --- | --- | --- |
| Версия | Класс трафика | Метка потока |
| Длина данных | Следующий заголовок | Счетчик сегментов |
| Адрес отправителя |
| Адрес получателя |

Рис. 3.2. Длина заголовка IPv6 фиксирована и равна 40 байтам

Следующие поля заголовка IPv4 были исключены из заголовка IPv6:

* + поля, относящиеся к фрагментации, такие как Fragment Offset (Смещение фрагмента) и Identification (Идентификатор), а также флаги Don't Fragment (Запрет фрагментации) и More Fragments (Флаг фрагментации);
	+ поле контрольной суммы;
	+ поле параметров.

Для увеличения скорости обработки пакетов в IPv6 было решено отказаться от их фрагментации. Очередной маршрутизатор, не способный передать дальше слишком большой пакет, не станет разбивать его на фрагменты, которые придется собирать на принимающем конце. Вместо этого пакет будет отброшен, а маршрутизатор вернет новое сообщение ICMP (Packet Too Big - слишком большой размер пакета) отправителю, который сможет самостоятельно разбить сообщение на более мелкие пакеты.

Дальнейшей попыткой увеличить скорость обработки пакетов в IPv6 является отказ от поля контрольной суммы пакета. Каждый маршрутизатор на пути пакета должен заново определять значение данного поля, так как счетчик сегментов в поле TTL уменьшается на каждом новом узле. Поскольку контрольная сумма вычисляется в лежащем в основе IP канальном уровне, а также в протоколах TCP и UDP, удаление этого поля из IP-заголовка не вызовет никаких проблем.

Новые сообщения ICMP

Протокол IP с помощью сообщений ICMP выполняет множество функций, наиболее известной из которых является проверка доступности узла удаленной сети утилитой PING, которая посылает для этого эхо сообщения ICMP. Как и протокол IP, ICMP будет расширен, чтобы идти в ногу со временем. Кроме изменений, связанных с введением IPv6, в ICMP будут включены функции протокола Internet Group Management Protocol (IGMP, протокола управления группами Internet).

С полем Options (Параметры) ситуация другая. Это поле переменной длины было убрано из IP-заголовка, чтобы его длина оказалась зафиксированной, но это не означает, что удалены также и параметры. Они могут быть заданы в поле Next Header (Следующий протокол), которое обычно обозначает другой протокол, такой как TCP или UDP. В этом случае параметры помещаются в область данных пакета, а в поле Next Header содержится указатель их положения. Благодаря отсутствию параметров в заголовке пакета (и тем самым сохранению длины заголовка постоянным) IP-пакеты обрабатываются намного быстрее.

В новом заголовок IPv6 могут содержаться следующие поля:

* Version (Версия) - 4-битное поле, обозначающее, как и в IPv4, версию протокола IP. В IPv6 всегда имеет значение 6;
* Traffic Class (Класс трафика) - 8-битное поле, предназначенное для тех же целей, что и поле Type of Service (Тип службы) в заголовке IPv4, хотя его спецификации еще не устоялись;
* Flow Label (Метка потока) - используется для обозначения различных потоков (flows) трафика. Позволяет задавать приоритеты обработки потоков. Окончательного определения потока еще нет. Это может быть более дорогостоящий трафик, либо трафик с аудио- или видеоданными;
* Payload Length (Длина данных) - 16-битное поле, указывающее число байт в блоке данных, который идет после заголовка;
* Next Header (Следующий заголовок) - служит для определения протокола более высокого уровня, которому IP передаст пакет для дальнейшей обработки. В данном поле применяются те же номера протоколов, что и в IPv4;
* Hop Limit (Счетчик сегментов) - максимально допустимое число сегментов. Каждый маршрутизатор, через который проходит пакет, уменьшает значение этого поля на единицу. Когда значение счетчика становится равным нулю, пакет отбрасывается;
* Source Address (Адрес отправителя) — 128-битное поле с адресом отправителя пакета;
* Destination Address (Адрес получателя) - 128-битное поле с адресом получателя пакета.

Расширенные заголовки

Поле Next Header в 40-байтном заголовке фиксированной длины служит для обозначения типа заголовка, который будет расположен в начале области данных IP-пакета. Вспомним, что внутри пакета IP обычно находится пакет протокола более высокого уровня, такого как TCP или UDP, который имеет собственный заголовок. За счет применения IP-заголовка фиксированной длины обработка пакетов на маршрутизаторах и других сетевых устройствах намного ускоряется. Но поскольку некоторые поля были исключены из заголовка, для выполнения их функций должны быть предусмотрены другие методы.

Поэтому было разработано несколько типов так называемых расширенных заголовков (extension headers), которые также могут находиться в начале области данных IP-пакета. При этом поле Next Header указывает на расширенный заголовок. В качестве подобных заголовков допускается указывать следующие:

* Hop-by-Hop Options (Параметры, проверяемые на каждом узле);
* Fragmentation (Фрагментация);
* Routing (Маршрутизация);
* Authentication (Аутентификация);
* Security Encapsulation (Защита содержания);
* Encapsulation Security Payload (Безопасное закрытие содержания);
* Destination Options (Параметры получателя).

Первый тип расширенного заголовка (проверяемые на каждом узле параметры) обозначается нулевым значением поля Next Header. В этом заголовке находится информация, которую должна контролировать каждая система на пути пакета. На настоящий момент определен лишь один подобный параметр - Jumbo Payload (Большой пакет), то есть IP-пакет размером более 65535 байт. Взглянув на формат расширенного заголовка (рис. 3.3), мы увидим, что он, как и заголовок IPv6, содержит поле Next Header. Это позволяет вводить несколько расширенных заголовков, каждый из которых указывает на следующий.

Расширенному заголовку Fragmentation соответствует значение поля Next Header, равное 44, и этот заголовок вводится в том случае, если отправитель пакета понимает, что для передачи по сети сообщение должно быть фрагментировано. IPv6 пакеты не фрагментируются - эта возможность была удалена для ускорения обработки IP-пакетов. Любая фрагментация сообщения выполняется отправителем пакета, и данный расширенный заголовок предназначен для хранения информации об этом процессе, чтобы принимающий узел был способен корректно собрать сообщение.

Следующий заголовок

Размер расширения заголовка

Параметры

8 бит

8 бит

Поле переменной длины

Рис. 3.3. Формат расширенного заголовка

Функции расширенного заголовка Routing (значение поля Next Header для которого равно 43) аналогичны маршрутизации от источника в IPv4. Здесь в заголовке задается один или несколько узлов, через которые должен пройти пакет на своем пути к месту назначения.

Расширенный заголовок Destinations Options (значение поля Next Header для которого равно 60) предназначен для записи информации, которую проверяет только получатель.

Значение 59 в поле Next Header говорит о том, что больше не осталось расширенных заголовков, которые необходимо проверить. Если размер области данных, указанный в поле Payload Length, превышает это значение, байты, оставшиеся после обнаружения заголовка с таким значением, будут игнорироваться.

Адресация IPv6

При переходе от 32 бит к 128 битам адресное пространство IPv6 астрономически увеличится по сравнению с IPv4.

В IPv6 существует три основных типа адресов:

* unicast (индивидуальный) - уникальный идентификатор определенного сетевого интерфейса;
* anycast (любой) - обозначает несколько интерфейсов. Пакет, направленный на адрес типа anycast, будет передан на ближайший интерфейс (определенный используемым протоколом маршрутизации), заданный этим адресом;
* multicast (групповой) - также указывает на несколько интерфейсов. Но в отличие от случая с адресом типа anycast, пакет, отправленный на адрес типа multicast, пересылается всем интерфейсам, обозначенным этим адресом.

Несмотря на то, что адрес типа unicast является уникальным идентификатором сетевого интерфейса, один интерфейс может иметь несколько unicast-адресов. Широковещательных (broadcast) адресов больше нет - их функциональность унаследовал тип адресов multicast.

# Заключения

Ознакомившись с описанными проблемами, можно сделать вывод, что межсетевые экраны обеспечивают защиту компьютерной сети организации от несанкционированного вмешательства. Межсетевые экраны являются необходимым средством обеспечения информационной безопасности. Они обеспечивают первую линию обороны. При выборе и приобретении межсетевых экранов необходимо тщательно все продумать и проанализировать. Выбрать нужную архитектуру и компонентов межсетевого экрана. Правильно настроить программную обеспечению и тестировать конфигурацию межсетевого экрана.

# Список сокращений и обозначений

|  |  |
| --- | --- |
| КСО | Компьютерный сеть организации |
| ИБ | Информационная безопасность |
| ОС | Операционная Система |
| ПО | Программное Обеспечение |
| НСД | Несанкционированный доступ |
| СОИБ | Система обеспечения информационной безопасности |
| СУБД | Система управлением база данных |
| ЦП | Центральный Процессор |
| CA | Certification Authority |
| CGI | Common Gateway Interface |
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | Demilitarized Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DSA | Digital Signature Algorithm |
| FTP | File Transport Protocol |
| GUI | Graphical User Interface |
| HTML | Hyper Text Markup Language |
| HTTP | Hyper Text Transfer Protocol |
| IDS | Intrusion Detection System |
| IIS | Internet Information Services |
| KSK | Key Signing Key |
| MAC | Media Access Control |
| MAC | Message Authentication Code |
| MD5 | Message Digest v5 |
| NAT | Network Address Translation |
| NTP | Network Time Protocol |
| NTP | Network Time Protocol |
| OSI | Open System Interconnection |
| PKI | Public Key Infrastructure |
| RSA | Rivest, Shamir, Adleman |
| SEP | Secure Entry Point |
| SHA | Secure Hash Algorithm |
| SMTP  | Simple Mail Transfer Protocol |
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| TOS | Trusted ОС |
| VPN | Virtual Private Network |
| URL | Uniform Resource Locator |
| REP | Robots Exclusion Standard |
| IE | Internet Explorer |
| SSI | Server Side Includes |
| ASP | Active Server Pages |
| ISP | Internet Service Provider |

#

# Список использованных источников литературы

1. О.Р. Лапонина. Межсетевое экранирование. «ИНТУИТ», М., 2009;
2. Т.В. Оглтри. Firewalls. Практические применение межсетевых экранов. «ДМК», М., 2008;
3. Девид Чемпен, Энди Фокс. Брандмауэры Cisco Secure PIX. «Вильямс», М., 2009;
4. Т.А. Биячуев. Безопасность корпоративных сетей. Спб., 2008;
5. А.Ю. Щеглов. Защита компьютерной сети от несанкционированного доступа. «НиТ», Спб., 2009;
6. Р. Зиглер. Брандмауэры в Linux. «Вильямс», М., 2009;
7. Журнал «Chip», июль 2007;
8. Журнал «Проблемы информационной безопасности», апрель 2008;
9. Яковлев. Лекция «Межсетевой экраны» 2009;

**Интернет ресурсы**

1. <http://securitylab.ru>
2. <http://cisco.com>
3. <http://zonealarm.com>
4. <http://hub.ru>
5. <http://opennet.ru>
6. <http://infosecurity.ru>
7. <http://osp.ru>
8. <http://www.security-teams.net>
9. <http://www.oszone.ru>
10. <http://www.secure.com.ru>