# Защита информации в глобальной сети

ПЛАН.

Введение.

Защита информации в глобальной сети.

1.    Проблема защиты информации.

2.    Информационная безопасность и информационные технологии.

3.    Средства защиты информации.

  3.1. Solstice Firewall-1.

   3.1.1. Назначение экранирующих систем и требования к ним.

   3.1.2. Структура системы Solstice Firewall-1.

   3.1.3. Пример реализации политики безопасности.

   3.1.4. Управление системой Firewall-1.

   3.1.5. Еще один пример реализации политики безопасности.

   3.1.6. Аутентификация пользователей при работе с FTP.

   3.1.7. Гибкие алгоритмы фильтрации UDP–пакетов, динамическое         экранирование.

3.1.8.    Язык программирования. Прозрачность и эффективность.

3.2.     Ограничение доступа в WWW серверах.

 3.2.1. Ограничения по IP–адресам.

 3.2.2. Ограничения по идентификатору получателя.

3.3.     Информационная безопасность в Intranet.

 3.3.1. Разработка сетевых аспектов политики безопасности.

 3.3.2. Процедурные меры.

 3.3.3. Управление доступом путем фильтрации информации.

 3.3.4. Безопасность программной среды.

 3.3.5. Защита Web–серверов.

 3.3.6. Аутентификация в открытых сетях.

 3.3.7.Простота и однородность архитектуры.

3.4. PGP.

3.5. Blowfish.

3.6. Kerberos.

4.    Виртуальные частные сети (VPN).

4.1.     Совместимость.

4.2.     Безопасность.

4.3.     Доступность.

4.4.     Управляемость.

4.5.     Архитектура VPN.

Заключение.

ВВЕДЕНИЕ.

Internet - глобальная компьютерная сеть, охватывающая весь мир. Сегодня Internet имеет около 15 миллионов абонентов в более чем 150 странах мира. Ежемесячно размер сети увеличивается на 7-10%. Internet образует как бы ядро, обеспечивающее связь различных информационных сетей, принадлежащих различным учреждениям  во всем  мире, одна с другой.

Если ранее сеть использовалась исключительно в качестве среды передачи файлов и сообщений электронной почты, то сегодня решаются более сложные задачи распределеного доступа к ресурсам. Около двух лет назад были созданы оболочки, поддерживающие функции сетевого поиска и доступа к распределенным информационным ресурсам, электронным архивам.

Internet, служившая когда-то исключительно исследовательским и учебным группам, чьи интересы простирались вплоть до доступа к суперкомпьютерам, становится все более популярной в деловом мире.

Компании соблазняют быстрота, дешевая глобальная связь, удобство для проведения совместных работ, доступные программы, уникальная база данных сети  Internet. Они рассматривают глобальную сеть как дополнение к своим собственным локальной сетям.

 Фактически Internet состоит из множества локальных и глобальных сетей, принадлежащих различным компаниям и предприятиям, связанных между собой различными линиями связи. Internet можно представить себе в виде мозаики сложенной из небольших сетей разной величины, которые активно взаимодействуют одна с другой, пересылая файлы, сообщения и т.п.

При низкой стоимости услуг (часто это только фиксированная ежемесячная плата за используемые линии или телефон) пользователи могут получить доступ к коммерческим и некоммерческим информационным службам США, Канады, Австралии и многих европейских стран. В архивах свободного доступа сети Internet можно найти информацию практически по всем сферам человеческой деятельности, начиная с новых научных открытий до прогноза погоды на завтра.

Кроме того Internet предоставляет уникальные возможности дешевой, надежной и конфиденциальной глобальной связи по всему миру. Это оказывается очень удобным для фирм имеющих свои филиалы по всему миру, транснациональных корпораций и структур управления. Обычно, использование инфраструктуры Internet для международной связи обходится значительно дешевле прямой компьютерной связи через спутниковый канал или через телефон.

Электронная почта - самая распространенная услуга сети Internet. В настоящее время свой адрес по электронной почте имеют приблизительно 20 миллионов человек. Посылка письма по электронной почте обходится значительно дешевле посылки обычного письма. Кроме того сообщение, посланное по электронной почте дойдет до адресата за несколько часов, в то время как обычное письмо может добираться до адресата несколько дней, а то и недель.

В настоящее время Internet испытывает период подъема, во многом благодаря активной поддержке со стороны правительств европейских стран и США. Ежегодно в США выделяется около 1-2 миллионов долларов на создание новой сетевой инфраструктуры. Исследования в области сетевых коммуникаций финансируются также правительствами Великобритании, Швеции, Финляндии, Германии.

Однако, государственное финансирование - лишь небольшая часть поступающих средств, т.к. все более заметной становится "коммерцизация" сети (80-90% средств поступает из частного сектора).

 Новые границы киберпространства открывают широкие возможности для новшеств, деловой активности и извлечения прибыли. Но есть у интерактивного мира и другая сторона - снижение степени безопасности корпораций. Сеть Internet породила нелегальный рынок, где сбывается информация, составляющая коммерческую тайну корпораций. По оценкам правоохранительных органов, интерактивные преступники ежегодно крадут информацию более чем на 10 млрд. долл. Однако закон до сих пор проигрывает в сражении с ними. Киберворы пользуются преимуществами, которые дает им система защиты Internet, включая свободно распространяемые алгоритмы шифрования с открытым ключом и анонимные узлы ретрансляции электронной почты. Эти средства служат укрытием для торговцев похищенной информацией во всем мире. Степень риска для корпораций повышается независимо от того, работают они по Internet или нет. Угрозу представляет не только возможность проникновения в корпоративную сеть через брандмауэр, но и само становление интерактивного рынка корпоративных данных, которые могут быть украдены и собственными сотрудниками компании.

Нелегальная деятельность по сети изменила лицо корпоративной службы безопасности. Раньше мог исчезнуть один ящик секретных сведений. Теперь же нетрудно скопировать и отправить по электронной почте эквивалент сотен таких ящиков. Все, что для этого требуется, - один хакер. В тот же вечер все сообщество хакеров будет в курсе дела. В число нелегально продаваемой и покупаемой информации входят номера талонов на телефонные переговоры, выдаваемых компаниями междугородной связи , коды подключения к службам сотовой связи, номера кредитных карточек, "вынюхивающие" алгоритмы взлома защиты и пиратские копии программного обеспечения. В некоторых случаях покупателями этой информации являются криминальные структуры, такие как продавцы пиратского ПО, которые покупают украденные номера талонов, чтобы бесплатно звонить по международному телефону. Что еще опаснее, на этом рынке распространяются коммерческие секреты организаций, в частности планы исследований и разработок компаний, занимающихся высокими технологиями. Хотя наибольшим атакам подвергаются сегодня телефонные службы и компании, выдающие кредитные карточки, повышение интенсивности интерактивной коммерции между крупными корпорациями может существенно увеличить риск электронных краж для всей промышленности. По мере выхода коммерции на информационную магистраль мы все становимся мишенями. Риску подвергаются программные агенты и другие объекты.

Распространение электронной коммерции приводит к созданию все новых интерактивных каналов связи, и нет гарантии, что любой из промежуточных каналов не окажется уязвимым местом с точки зрения защиты. Конечно, в краже коммерческих секретов нет ничего нового. Но Internet и другие интерактивные службы открывают торговцам информацией новые возможности для поиска и обмена данными.

.

**Защита информации в глобальной сети Internet.**

***1.Проблемы защиты информации.***

            Internet и информационная безопасность несовместны по самой природе Internet. Она родилась как чисто корпоративная сеть, однако, в настоящее время с помощью единого стека протоколов TCP/IP и единого адресного пространства объединяет не только корпоративные и ведомственные сети (образовательные, государственные, коммерческие, военные и т.д.), являющиеся, по определению, сетями с ограниченным доступом, но и рядовых пользователей, которые имеют возможность получить прямой доступ в Internet со своих домашних компьютеров с помощью модемов и телефонной сети общего пользования.

            Как известно, чем проще доступ в Сеть, тем хуже ее информационная безопасность, поэтому с полным основанием можно сказать, что изначальная простота доступа в Internet - хуже воровства, так как пользователь может даже и не узнать, что у него были скопированы - файлы и программы, не говоря уже о возможности их порчи и корректировки.

            Что же определяет бурный рост Internet, характеризующийся ежегодным удвоением числа пользователей? Ответ прост -“халява”, то есть дешевизна программного обеспечения (TCP/IP), которое в настоящее время включено в Windows 95, легкость и дешевизна доступа в Internet (либо с помощью IP-адреса, либо с помощью провайдера) и ко всем мировым информационным ресурсам.

            Платой за пользование Internet является всеобщее снижение информационной безопасности, поэтому для предотвращения несанкционированного доступа к своим компьютерам все корпоративные и ведомственные сети, а также предприятия, использующие технологию intranet, ставят фильтры (fire-wall) между внутренней сетью и Internet, что фактически означает выход из единого адресного пространства. Еще большую безопасность даст отход от протокола TCP/IP и доступ в Internet через шлюзы.

            Этот переход можно осуществлять одновременно с процессом построения всемирной информационной сети общего пользования, на базе использования сетевых компьютеров, которые с помощью сетевой карты 10Base-T и кабельного модема обеспечивают высокоскоростной доступ (10 Мбит/с) к локальному Web-серверу через сеть кабельного телевидения.

            Для решения этих и других вопросов при переходе к новой архитектуре Internet нужно предусмотреть следующее:

**Во-первых**, ликвидировать физическую связь между будущей Internet (которая превратится во Всемирную информационную сеть общего пользования) и корпоративными и ведомственными сетями, сохранив между ними лишь информационную связь через систему World Wide Web.

**Во-вторых**, заменить маршрутизаторы на коммутаторы, исключив обработку в узлах IP-протокола и заменив его на режим трансляции кадров Ethernet, при котором процесс коммутации сводится к простой операции сравнения MAC-адресов.

**В-третьих**, перейти в новое единое адресное пространство на базе физических адресов доступа к среде передачи (MAC-уровень), привязанное к географическому расположению сети, и позволяющее в рамках 48-бит создать адреса для более чем 64 триллионов независимых узлов.

            Безопасность данных является одной из главных проблем в Internet.  Появляются все новые и новые страшные истории о том, как компьютерные взломщики, использующие все более изощренные приемы, проникают в чужие базы данных. Разумеется, все это не способствует популярности Internet в деловых кругах. Одна только мысль о том, что какие-нибудь хулиганы или, что еще хуже, конкуренты, смогут получить доступ к архивам коммерческих данных, заставляет руководство корпораций отказываться от использования открытых информационных систем. Специалисты утверждают, что подобные опасения безосновательны, так как у компаний, имеющих доступ и к открытым, и частным сетям, практически равные шансы стать жертвами компьютерного террора.

Дилемма безопасности такова: приходится делать выбор между защищенностью вашего имущества и его доступностью для вас, а значит, и возможностью полезного использования.

            Это справедливо и в отношении информации. Например, база данных, содержащая конфиденциальные сведения, лишь тогда полностью защищена от посягательств, когда она находится на дисках, снятых с компьютера и убранных в охраняемое место. Как только вы установили эти диски в компьютер и начали использовать, появляется сразу несколько каналов, по которым злоумышленник, в принципе, имеет возможность получить к вашим тайнам доступ без вашего ведома. Иными словами, ваша информация либо недоступна для всех, включая и вас, либо не защищена на сто процентов.

            В области информации дилемма безопасности формулируется следующим образом: следует выбирать между защищенностью системы и ее открытостью. Правильнее, впрочем, говорить не о выборе, а о балансе, так как система, не обладающая свойством открытости, не может быть использована.

            В банковской сфере проблема безопасности информации осложняется двумя факторами: во-первых, почти все ценности, с которыми имеет дело банк (кроме наличных денег и еще кое-чего), существуют лишь в виде той или иной информации. Во-вторых, банк не может существовать без связей с внешним миром: без клиентов, корреспондентов и т. п. При этом по внешним связям обязательно передается та самая информация, выражающая собой ценности, с которыми работает банк (либо сведения об этих ценностях и их движении, которые иногда стоят дороже самих ценностей). Извне приходят документы, по которым банк переводит деньги с одного счета на другой. Вовне банк передает распоряжения о движении средств по корреспондентским счетам, так что открытость банка задана a priori.

2. Информационная безопасность и информационные технологии

            На раннем этапе автоматизации внедрение банковских систем (и вообще средств автоматизации банковской деятельности) не повышало открытость банка.  Общение с внешним миром, как и прежде, шло через операционистов и курьеров, поэтому дополнительная угроза безопасности информации проистекала лишь от возможных злоупотреблений со стороны работавших в самом банке специалистов по информационным технологиям.

            Положение изменилось после того, как на рынке финансовых услуг стали появляться продукты, само возникновение которых было немыслимо без информационных технологий. В первую очередь это—пластиковые карточки.  Пока обслуживание по карточкам шло в режиме голосовой авторизации, открытость информационной системы банка повышалась незначительно, но затем появились банкоматы, POS-терминалы, другие устройства самообслуживания—то есть средства, принадлежащие к информационной системе банка, но расположенные вне ее и доступные посторонним для банка лицам.

            Повысившаяся открытость системы потребовала специальных мер для контроля и регулирования обмена информацией: дополнительных средств идентификации и аутентификации лиц, которые запрашивают доступ к системе (PIN-код, информация о клиенте на магнитной полосе или в памяти микросхемы карточки, шифрование данных, контрольные числа и другие средства защиты карточек), средств криптозащиты информации в каналах связи и т. д.

            Еще больший сдвиг баланса “защищенность-открытость” в сторону последней связан с телекоммуникациями. Системы электронных расчетов между банками защитить относительно несложно, так как субъектами электронного обмена информацией выступают сами банки. Тем не менее, там, где защите не уделялось необходимое внимание, результаты были вполне предсказуемы.  Наиболее кричащий пример—к сожалению, наша страна. Использование крайне примитивных средств защиты телекоммуникаций в 1992 г. привело к огромным потерям на фальшивых авизо.

            Общая тенденция развития телекоммуникаций и массового распространения вычислительной техники привела в конце концов к тому, что на рынке банковских услуг во всем мире появились новые, чисто телекоммуникационные продукты, и в первую очередь системы Home Banking (отечественный аналог—“клиент-банк”). Это потребовало обеспечить клиентам круглосуточный доступ к автоматизированной банковской системе для проведения операций, причем полномочия на совершение банковских транзакций получил непосредственно клиент. Степень открытости информационной системы банка возросла почти до предела. Соответственно, требуются особые, специальные меры для того, чтобы столь же значительно не упала ее защищенность.

            Наконец, грянула эпоха “информационной супермагистрали”: взрывообразное развитие сети Internet и связанных с нею услуг. Вместе с новыми возможностями эта сеть принесла и новые опасности. Казалось бы, какая разница, каким образом клиент связывается с банком: по коммутируемой линии, приходящей на модемный пул банковского узла связи, или по IP-протоколу через Internet? Однако в первом случае максимально возможное количество подключений ограничивается техническими характеристиками модемного пула, во втором же—возможностями Internet, которые могут быть существенно выше.  Кроме того, сетевой адрес банка, в принципе, общедоступен, тогда как телефонные номера модемного пула могут сообщаться лишь заинтересованным лицам. Соответственно, открытость банка, чья информационная система связана с Internet, значительно выше, чем в первом случае. Так только за пять месяцев 1995 г. компьютерную сеть Citicorp взламывали 40 раз! (Это свидетельствует, впрочем, не столько о какой-то “опасности” Internet вообще, сколько о недостаточно квалифицированной работе администраторов безопасности Citicorp.)

            Все это вызывает необходимость пересмотра подходов к обеспечению информационной безопасности банка. Подключаясь к Internet, следует заново провести анализ риска и составить план защиты информационной системы, а также конкретный план ликвидации последствий, возникающих в случае тех или иных нарушений конфиденциальности, сохранности и доступности информации.

            На первый взгляд, для нашей страны проблема информационной безопасности банка не столь остра: до Internet ли нам, если в большинстве банков стоят системы второго поколения, работающие в технологии “файл-сервер”. К сожалению, и у нас уже зарегистрированы “компьютерные кражи”. Положение осложняется двумя проблемами. Прежде всего, как показывает опыт общения с представителями банковских служб безопасности, и в руководстве, и среди персонала этих служб преобладают бывшие оперативные сотрудники органов внутренних дел или госбезопасности. Они обладают высокой квалификацией в своей области, но в большинстве своем слабо знакомы с информационными технологиями. Специалистов по информационной безопасности в нашей стране вообще крайне мало, потому что массовой эта профессия становится только сейчас.

Вторая проблема связана с тем, что в очень многих банках безопасность автоматизированной банковской системы не анализируется и не обеспечивается всерьез. Очень мало где имеется тот необходимый набор организационных документов (анализ риска, план защиты и план ликвидации последствий), о котором говорилось выше. Более того, безопасность информации сплошь и рядом просто не может быть обеспечена в рамках имеющейся в банке автоматизированной системы и принятых правил работы с ней.

            Что касается автоматизированных банковских систем, то наиболее распространенные системы второго-третьего поколений состоят из набора автономных программных модулей, запускаемых из командной строки DOS на рабочих станциях. Оператор имеет возможность в любой момент выйти в DOS из такого программного модуля. Предполагается, что это необходимо для перехода в другой программный модуль, но фактически в такой системе не существует никаких способов не только исключить запуск оператором любых других программ (от безобидной игры до программы, модифицирующей данные банковских счетов), но и проконтролировать действия оператора. Стоит заметить, что в ряде систем этих поколений, в том числе разработанных весьма уважаемыми отечественными фирмами и продаваемых сотнями, файлы счетов не шифруются, т.  е. с данными в них можно ознакомиться простейшими общедоступными средствами. Многие разработчики ограничивают средства администрирования безопасности штатными средствами сетевой операционной системы: вошел в сеть - делай, что хочешь.

            Тем не менее, наши банки уделяют информационным технологиям много внимания, и достаточно быстро усваивают новое. Сеть Internet и финансовые продукты, связанные с ней, войдут в жизнь банков быстрее, чем это предполагают скептики, поэтому уже сейчас необходимо озаботиться вопросами информационной безопасности на другом, более профессиональном уровне, чем это делалось до сих пор.

Некоторые рекомендации:

1. Необходим комплексный подход к информационной безопасности.

Информационная безопасность должна рассматриваться как составная часть общей безопасности банка—причем как важная и неотъемлемая ее часть.  Разработка концепции информационной безопасности должна обязательно проходить при участии управления безопасности банка. В этой концепции следует предусматривать не только меры, связанные с информационными технологиями (криптозащиту, программные средства администрирования прав пользователей, их идентификации и аутентификации, “брандмауэры” для защиты входов—выходов сети и т. п.), но и меры административного и технического характера, включая жесткие процедуры контроля физического доступа к автоматизированной банковской системе.

2. Необходимо участие сотрудников управления безопасности на этапе выбора—приобретения—разработки автоматизированной банковской системы. Это участие не должно сводиться к проверке фирмы-поставщика. Управление безопасности должно контролировать наличие надлежащих средств разграничения доступа к информации в приобретаемой системе.

3.Средства защиты информации.

            Сейчас вряд ли кому-то надо доказывать, что при подключении к Internet Вы подвергаете риску безопасность Вашей локальной сети и конфиденциальность содержащейся в ней информации. По данным CERT Coordination Center в 1995 году было зарегистрировано 2421 инцидентов - взломов локальных сетей и серверов. По результатам опроса, проведенного Computer Security Institute (CSI) среди 500 наиболее крупных организаций, компаний и университетов с 1991 число незаконных вторжений возросло на 48.9 %, а потери, вызванные этими атаками, оцениваются в 66 млн. долларов США.

            Одним из наиболее распространенных механизмов защиты от интернетовских бандитов - “хакеров” является применение межсетевых экранов - **брэндмауэров (firewalls).**

            Стоит отметить, что вследствие непрофессионализма администраторов и недостатков некоторых типов брэндмауэров порядка 30% взломов совершается после установки защитных систем.

**3.1 Технология работы в глобальных сетях Solstice FireWall-1 .**

            В настоящее время вопросам безопасности данных в распределенных компьютерных системах уделяется очень большое внимание. Разработано множество средств для обеспечения информационной безопасности, предназначенных для использования на различных компьютерах с разными ОС. В качестве одного из направлений можно выделить межсетевые экраны (firewalls), призванные контролировать доступ к информации со стороны пользователей внешних сетей.

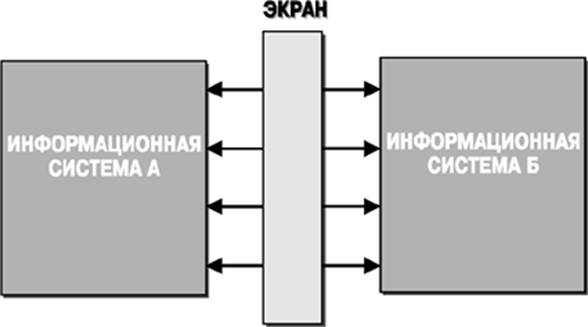
            В настоящем документе рассматриваются основные понятия экранирующих систем, а также требования, предъявляемые к ним. На примере пакета Solstice FireWall-1 рассматривается неcколько типичных случаев использования таких систем, особенно применительно к вопросам обеспечения безопасности Internet-подключений. Рассмотрено также несколько уникальных особенностей Solstice FireWall-1, позволяющих говорить о его лидерстве в данном классе приложений.

***3.1.1. НАЗНАЧЕНИЕ ЭКРАНИРУЮЩИХ СИСТЕМ И ТРЕБОВАНИЯ К НИМ***

***.***

            Проблема межсетевого экранирования формулируется следующим образом. Пусть имеется две информационные системы или два множества информационных систем.  Экран (firewall) - это средство разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве.

Рисунок 3.1.1.1



            Экран FireWall.

            Экран выполняет свои функции, контролируя все информационные потоки между этими двумя множествами информационных систем, работая как некоторая “информационная мембрана”. В этом смысле экран можно представлять себе как набор фильтров, анализирующих проходящую через них информацию и, на основе заложенных в них алгоритмов, принимающих решение: пропустить ли эту информацию или отказать в ее пересылке. Кроме того, такая система может выполнять регистрацию событий, связанных с процессами разграничения доступа. в частности, фиксировать все “незаконные” попытки доступа к информации и, дополнительно, сигнализировать о ситуациях, требующих немедленной реакции, то есть поднимать тревогу.

            Обычно экранирующие системы делают несимметричными. Для экранов определяются понятия “внутри” и “снаружи”, и задача экрана состоит в защите внутренней сети от “потенциально враждебного” окружения. Важнейшим примером потенциально враждебной внешней сети является Internet.

            Рассмотрим более подробно, какие проблемы возникают при построении экранирующих систем. При этом мы будем рассматривать не только проблему безопасного подключения к Internet, но и разграничение доступа внутри корпоративной сети организации.

**Первое,** очевидное требование к таким системам, это обеспечение безопасности внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи.

**Во-вторых,** экранирующая система должна обладать мощными и гибкими средствами управления для простого и полного воплощения в жизнь политики безопасности организации и, кроме того, для обеспечения простой реконфигурации системы при изменении структуры сети.

**В-третьих,** экранирующая система должна работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий.

**В-четвертых,** экранирующая система должна работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик в “пиковых” режимах.  Это необходимо для того, чтобы firewall нельзя было, образно говоря, “забросать” большим количеством вызовов, которые привели бы к нарушению ее работы.

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

**Шестое.** В идеале, если у организации имеется несколько внешних подключений, в том числе и в удаленных филиалах, система управления экранами должна иметь возможность централизованно обеспечивать для них проведение единой политики безопасности.

**Седьмое.** Система Firewall должна иметь средства авторизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать, например, в командировки, и в процессе работы им, тем немение, требуется доступ, по крайней мере, к некоторым ресурсам внутренней компьютерной сети организации. Система должна уметь надежно распознавать таких пользователей и предоставлять им необходимый доступ к информации.

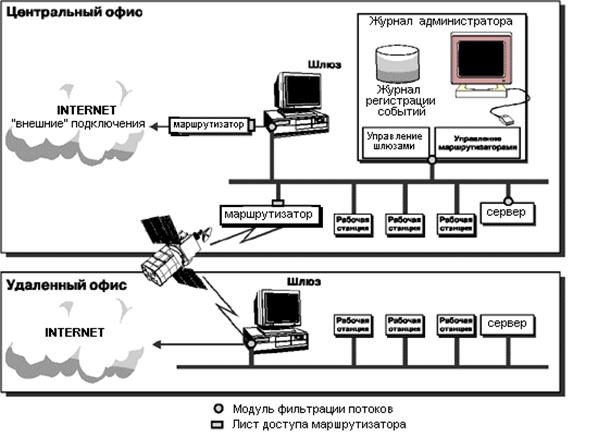
***3.1.2. СТРУКТУРА СИСТЕМЫ SOLSTICE FIREWALL-1.***

            Классическим примером, на котором хотелось бы проиллюстрировать все вышеизложенные принципы, является программный комплекс Solstice FireWall-1 компании Sun Microsystems. Данный пакет неоднократно отмечался наградами на выставках и конкурсах. Он обладает многими полезными особенностями, выделяющими его среди продуктов аналогичного назначения.

            Рассмотрим основные компоненты Solstice FireWall-1 и функции, которые они реализуют.

            Центральным для системы FireWall-1 является модуль управления всем комплексом. С этим модулем работает администратор безопасности сети.  Следует отметить, что продуманность и удобство графического интерфейса модуля управления отмечалось во многих независимых обзорах, посвященных продуктам данного класса.

*Рисунок 3.1.2.1*



            Основные компоненты Solstice FireWall-1 .

            Администратору безопасности сети для конфигурирования комплекса FireWall-1 необходимо выполнить следующий ряд действий:

•          Определить объекты, участвующие в процессе обработки информации. Здесь имеются в виду пользователи и группы пользователей, компьютеры и их группы, маршрутизаторы и различные подсети локальной сети организации.

•          Описать сетевые протоколы и сервисы, с которыми будут работать приложения. Впрочем, обычно достаточным оказывается набор из более чем 40 описаний, поставляемых с системой FireWall-1.

•          Далее, с помощью введенных понятий описывается политика разграничения доступа в следующих терминах: “Группе пользователей А разрешен доступ к ресурсу Б с помощью сервиса или протокола С, но об этом необходимо сделать пометку в регистрационном журнале”. Совокупность таких записей компилируется в исполнимую форму блоком управления и далее передается на исполнение в модули фильтрации.

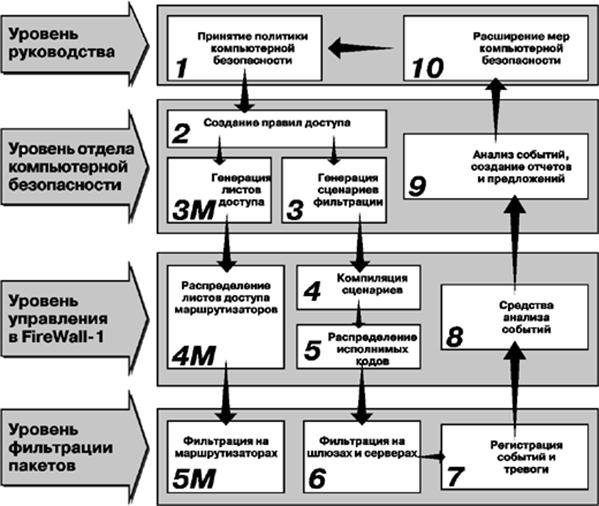
            Модули фильтрации могут располагаться на компьютерах - шлюзах или выделенных серверах - или в маршрутизаторах как часть конфигурационной информации. В настоящее время поддерживаются следующие два типа маршрутизаторов: Cisco IOS 9.x, 10.x, а также BayNetworks (Wellfleet) OS v.8.

            Модули фильтрации просматривают все пакеты, поступающие на сетевые интерфейсы, и, в зависимости от заданных правил, пропускают или отбрасывают эти пакеты, с соответствующей записью в регистрационном журнале. Следует отметить, что эти модули, работая непосредственно с драйверами сетевых интерфейсов, обрабатывают весь поток данных, располагая полной информацией о передаваемых пакетах.

***3.1.3. ПРИМЕР РЕАЛИЗАЦИИ ПОЛИТИКИ БЕЗОПАСНОСТИ.***

            Расcмотрим процесc практической реализации политики безопасности организации с помощью программного пакета FireWall-1.

*Рисунок.3.1.3..1*



            Реализация политики безопасности FireWall.

1. Прежде всего, как уже отмечалось, разрабатываются и утверждаются на уровне руководства организации правила политики безопасности.

2. После утверждения эти правила надо воплотить в жизнь. Для этого их нужно перевести в структуру типа “откуда, куда и каким способом доступ разрешен или, наоборот, запрещен. Такие структуры, как мы уже знаем, легко переносятся в базы правил системы FireWall-1.

3. Далее, на основе этой базы правил формируются списки доступа для маршрутизаторов и сценарии работы фильтров на сетевых шлюзах. Списки и сценарии далее переносятся на физические компоненты сети, после чего правила политики безопасности “вступают в силу”.

4. В процессе работы фильтры пакетов на шлюзах и серверах генерируют записи обо всех событиях, которые им приказали отслеживать, а, также, запускают механизмы “тревоги”, требующие от администратора немедленной реакции.

5. На основе анализа записей, сделанных системой, отдел компьютерной безопасности организации может разрабатывать предложения по изменению и дальнейшему развитию политики безопасности.

Рассмотрим простой пример реализации следующих правил:

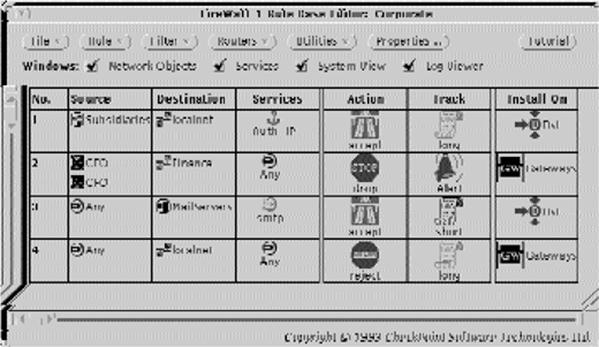
1. Из локальных сетей подразделений, возможно удаленных, разрешается связь с любой локальной сетью организации после аутентификации, например, по UNIX-паролю.

2. Всем запрещается доступ к сети финансового департамента, за исключением генерального директора и директора этого департамента.

3. Из Internet разрешается только отправлять и получать почту. Обо всех других попытках связи необходимо делать подробную запись.

            Все эти правила естественным образом представляются средствами графического интерфейса Редактора Правил FireWall-1.

Р*исунок 3.1.3..2*



                        Графический интерфейс Редактора Правил  FireWall-1 .

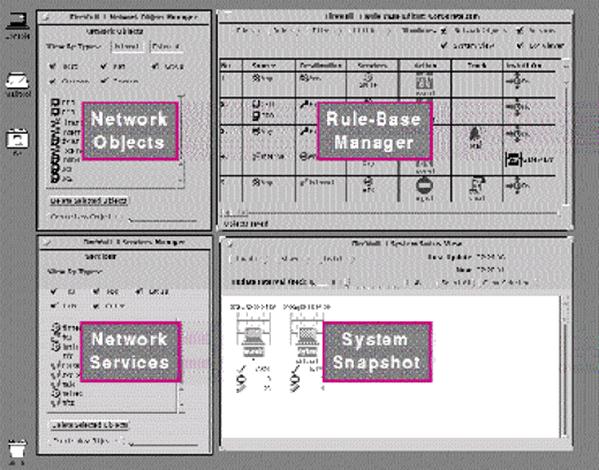
            После загрузки правил, FireWall-1 для каждого пакета, передаваемого по сети, последовательно просматривает список правил до нахождения элемента, соответствующего текущему случаю.

            Важным моментом является защита системы, на которой размещен административно-конфигурационный модуль FireWall-1. Рекомендуется запретить средствами FireWall-1 все виды доступа к данной машине, или по крайней мере строго ограничить список пользователей, которым это разрешено, а также принять меры по физическому ограничению доступа и по защите обычными средствами ОС UNIX.

***3.1.4.УПРАВЛЕНИЕ СИСТЕМОЙ FIREWALL-1 .***

 На рис. 5 показаны основные элементы управления системой FireWall-1.

*Рисунок. 3.1.4.1*



                        Основные элементы управления системой FireWall-1.

            Слева расположены редакторы баз данных об объектах, существующих в сети и о протоколах или сервисах, с помощью которых происходит обмен информацией.  Справа вверху показан редактор правил доступа.

            Справа внизу располагается интерфейс контроля текущего состояния системы, в котором для всех объектов, которые занес туда администратор, отображаются данные о количестве разрешенных коммуникаций (галочки), о количестве отвергнутых связей (знак “кирпич”) и о количестве коммуникаций с регистрацией (иконка карандаш). Кирпичная стена за символом объекта (компьютера) означает, что на нем установлен модуль фильтрации системы FireWall-1.

***3.1.5. ЕЩЕ ОДИН ПРИМЕР РЕАЛИЗАЦИИ ПОЛИТИКИ БЕЗОПАСНОСТИ.***

            Рассмотрим теперь случай, когда первоначальная конфигурация сети меняется, а вместе с ней меняется и политика безопасности.

            Пусть мы решили установить у себя в организации несколько общедоступных серверов для предоставления информационных услуг. Это могут быть, например, серверы World Wide Web, FTP или другие информационные серверы. Поскольку такие системы обособлены от работы всей остальной сети организации, для них часто выделяют свою собственную подсеть, имеющую выход в Internet через шлюз.

*Рисунок 3.1.5.1*

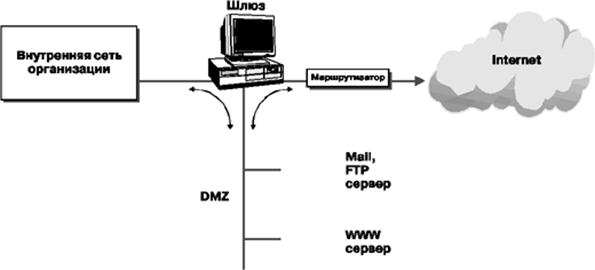


            Схема шлюза Internet.

            Поскольку в предыдущем примере локальная сеть была уже защищена, то все, что нам надо сделать, это просто разрешить соответствующий доступ в выделенную подсеть. Это делается с помощью одной дополнительной строки в редакторе правил, которая здесь показана. Такая ситуация является типичной при изменении конфигурации FireWall-1. Обычно для этого требуется изменение одной или небольшого числа строк в наборе правил доступа, что, несомненно, иллюстрирует мощь средств конфигурирования и общую продуманность архитектуры FireWall-1.

***3.1.6. АУТЕНФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ С FTP.***

            Solstice FireWall-1 позволяет администратору установить различные режимы работы с интерактивными сервисами FTP и telnet для различных пользователей и групп пользователей. При установленном режиме аутентификации, FireWall-1 заменяет стандартные FTP и telnet демоны UNIX на свои собственные, располагая их на шлюзе, закрытом с помощью модулей фильтрации пакетов.  Пользователь, желающий начать интерактивную сессию по FTP или telnet (это должен быть разрешенный пользователь и в разрешенное для него время), может сделать это только через вход на такой шлюз, где и выполняется вся процедура аутентификации. Она задается при описании пользователей или групп пользователей и может проводиться следующими способами:

•          Unix-пароль;

•          программа S/Key генерации одноразовых паролей;

•          карточки SecurID с аппаратной генерацией одноразовых паролей.

***3.1.7. ГИБКИЕ АЛГОРИТМЫ ФИЛЬТРАЦИИ UDP-ПАКЕТОВ, ДИНАМИЧЕСКОЕ ЭКРАНИРОВАНИЕ.***

            UDP-протоколы, входящие в состав набора TCP/IP, представляют собой особую проблему для обеспечения безопасности. С одной стороны на их основе создано множество приложений. С другой стороны, все они являются протоколами “без состояния”, что приводит к отсутствию различий между запросом и ответом, приходящим извне защищаемой сети.

            Пакет FireWall-1 решает эту проблему созданием контекста соединений поверх UDP сессий, запоминая параметры запросов. Пропускаются назад только ответы внешних серверов на высланные запросы, которые однозначно отличаются от любых других UDP-пакетов (читай: незаконных запросов), поскольку их параметры хранятся в памяти FireWall-1.

            Следует отметить, что данная возможность присутствует в весьма немногих программах экранирования, распространяемых в настоящий момент.

            Заметим также, что подобные механизмы задействуются для приложений, использующих RPC, и для FTP сеансов. Здесь возникают аналогичные проблемы, связанные с динамическим выделением портов для сеансов связи, которые FireWall-1 отслеживает аналогичным образом, запоминая необходимую информацию при запросах на такие сеансы и обеспечивая только “законный” обмен данными.

Данные возможности пакета Solstice FireWall-1 резко выделяют его среди всех остальных межсетевых экранов. Впервые проблема обеспечения безопасности решена для всех без исключения сервисов и протоколов, существующих в Internet.

***3.1.8. ЯЗЫК ПРОГРАММИРОВАНИЯ. ПРОЗРАЧНОСТЬ И ЭФФЕКТИВНОСТЬ.***

            Система Solstice FireWall-1 имеет собственный встроенный обьектно-ориентированный язык программирования, применяемый для описания поведения модулей - Фильтров системы. Собственно говоря, результатом работы графического интерфейса администратора системы является сгенерированный сценарий работы именно на этом внутреннем языке. Он не сложен для понимания, что допускает непосредственное программирование на нем. Однако на практике данная возможность почти не используется, поскольку графический интерфейс системы и так позволяет сделать практически все, что нужно.

            FireWall-1 полностью прозрачен для конечных пользователей. Еще одним замечательным свойством системы Solstice FireWall-1 является очень высокая скорость работы. Фактически модули системы работают на сетевых скоростях передачи информации, что обусловлено компиляцией сгенерированных сценариев работы перед подключением их непосредственно в процесс фильтрации.

            Компания Sun Microsystems приводит такие данные об эффективности работы Solstice FireWall-1. Модули фильтрации на Internet-шлюзе, сконфигурированные типичным для многих организаций образом, работая на скоростях обычного Ethernet в 10 Мб/сек, забирают на себя не более 10% вычислительной мощности процессора SPARCstation 5,85 МГц или компьютера 486DX2-50 с операционной системой Solaris/x86.

Solstice FireWall-1 - эффективное средство защиты корпоративных сетей и их сегментов от внешних угроз, а также от несанкционированных взаимодействий локальных пользователей с внешними системами.

Solstice FireWall-1 обеспечивает высокоуровневую поддержку политики безопасности организации по отношению ко всем протоколам семейства TCP/IP.

Solstice FireWall-1 характеризуется прозрачностью для легальных пользователей и высокой эффективностью.

По совокупности технических и стоимостных характеристик Solstice FireWall-1 занимает лидирующую позицию среди межсетевых экранов.

**3.2. Ограничения доступа в WWW серверах.**

Рассмотрим два из них:

•          Ограничить доступ по IP адресам клиентских машин;

•          ввести идентификатор получателя с паролем для данного вида документов.

Такого рода ввод ограничений стал использоваться достаточно часто, т.к.  многие стремятся в Internet, чтобы использовать его коммуникации для доставки своей информации потребителю. С помощью такого рода механизмов по разграничению прав доступа удобно производить саморассылку информации на получение которой существует договор.

***3.2.1. Ограничения по IP адресам.***

Доступ к приватным документам можно разрешить, либо наоборот запретить используя IP адреса конкретных машин или сеток, например:

                               123.456.78.9

                                123.456.79.

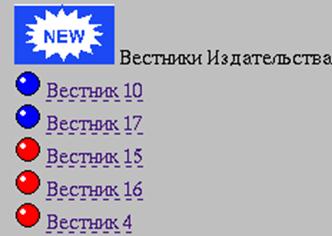
В этом случае доступ будет разрешен (или запрещен в зависимости от контекста) для машины с IP адресом 123.456.78.9 и для всех машин подсетки 123.456.79.

***3.2.2. Ограничения по идентификатору получателя.***

Доступ к приватным документам можно разрешить, либо наоборот запретить используя присвоенное имя и пароль конкретному пользователю, причем пароль в явном виде нигде не хранится.

Рассмотрим такой пример: Агенство печати предоставляет свою продукцию, только своим подписчикам, которые заключили договор и оплатили подписку.  WWW Сервер находится в сети Internet и общедоступен.

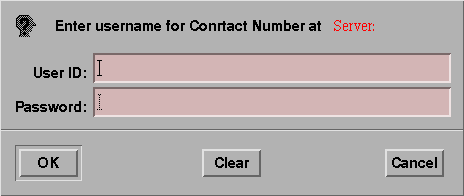
*Рисунок 3.2.2.1*



            Пример списка вестников издательства.

            Выберем Вестник предоставляемый конкретному подписчику. На клиентском месте подписчик получает сообщение:

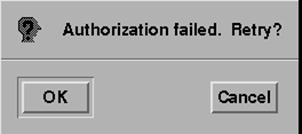
*Рисунок.3.2.2.2*



            Окно ввода пароля.

            Если он правильно написал свое имя и пароль, то он допускается до документа, в противном случае - получает сообщение:

*Рисунок.3.2.2.3*



            Окно неправильного ввода пароля.

**3.3 Информационная безопасность в Intranet.**

            Архитектура Intranet подразумевает подключение к внешним открытым сетям, использование внешних сервисов и предоставление собственных сервисов вовне, что предъявляет повышенные требования к защите информации.

            В Intranet-системах используется подход клиент-сервер, а главная роль на сегодняшний день отводится Web-сервису. Web-серверы должны поддерживать традиционные защитные средства, такие как аутентификация и разграничение доступа; кроме того, необходимо обеспечение новых свойств, в особенности безопасности программной среды и на серверной, и на клиентской сторонах.

            Таковы, если говорить совсем кратко, задачи в области информационной безопасности, возникающие в связи с переходом на технологию Intranet. Далее мы рассмотрим возможные подходы к их решению.

Формирование режима информационной безопасности - проблема комплексная.

Меры по ее решению можно разделить на четыре уровня:

•  законодательный (законы, нормативные акты, стандарты и т.п.);

•  административный (действия общего характера, предпринимаемые руководством организации);

•  процедурный (конкретные меры безопасности, имеющие дело с людьми);

•  программно-технический (конкретные технические меры).

***3.3.1. РАЗРАБОТКА СЕТЕВЫХ АСПЕКТОВ ПОЛИТИКИ БЕЗОПАСНОСТИ.***

            Политика безопасности определяется как совокупность документированных

управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

•  невозможность миновать защитные средства;

•  усиление самого слабого звена;

•  невозможность перехода в небезопасное состояние;

•  минимизация привилегий;

•  разделение обязанностей;

•  эшелонированность обороны;

•  разнообразие защитных средств;

•  простота и управляемость информационной системы;

•  обеспечение всеобщей поддержки мер безопасности.

            Поясним смысл перечисленных принципов.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Применительно к межсетевым экранам данный принцип означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через экран. Не должно быть “тайных” модемных входов или тестовых линий, идущих в обход экрана.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью.  Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

**Принцип невозможности** перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

**Принцип минимизации** привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

**Принцип разделения** обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

**Принцип эшелонированности обороны** предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

**Принцип разнообразия защитных средств** рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

**Очень важен принцип простоты** и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс.  Соответственно, если объекты некоторого вида (скажем таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудноуправляемой.

**Последний принцип** - всеобщая поддержка мер безопасности - носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

            Анализ рисков - важнейший этап выработки политики безопасности. При оценке рисков, которым подвержены Intranet-системы, нужно учитывать следующие обстоятельства:

•  новые угрозы по отношению к старым сервисам, вытекающие из возможности пассивного или активного прослушивания сети. Пассивное прослушивание означает чтение сетевого трафика, а активное - его изменение (кражу, дублирование или модификацию передаваемых данных). Например, аутентификация удаленного клиента с помощью пароля многократного использования не может считаться надежной в сетевой среде, независимо от длины пароля;

•  новые (сетевые) сервисы и ассоциированные с ними угрозы.

            Как правило, в Intranet-системах следует придерживаться принципа “все, что не разрешено, запрещено”, поскольку “лишний” сетевой сервис может предоставить канал проникновения в корпоративную систему. В принципе, ту же мысль выражает положение “все непонятное опасно”.

***3.3.1. ПРОЦЕДУРНЫЕ МЕРЫ.***

            В общем и целом Intranet-технология не предъявляет каких-либо специфических требований к мерам процедурного уровня. На наш взгляд, отдельного рассмотрения заслуживают лишь два обстоятельства:

•  описание должностей, связанных с определением, наполнением и поддержанием корпоративной гипертекстовой структуры официальных документов;

•  поддержка жизненного цикла информации, наполняющей Intranet.

            При описании должностей целесообразно исходить из аналогии между Intranet и издательством. В издательстве существует директор, определяющий общую направленность деятельности. В Intranet ему соответствует Web-администратор, решающий, какая корпоративная информация должна присутствовать на Web-сервере и как следует структурировать дерево (точнее, граф) HTML-документов.

            В многопрофильных издательствах существуют редакции, занимающиеся конкретными направлениями (математические книги, книги для детей и т.п.).  Аналогично, в Intranet целесообразно выделить должность публикатора, ведающего появлением документов отдельных подразделений и определяющего перечень и характер публикаций.

            У каждой книги есть титульный редактор, отвечающий перед издательством за свою работу. В Intranet редакторы занимаются вставкой документов в корпоративное дерево, их коррекцией и удалением. В больших организациях “слой” публикатор/редактор может состоять из нескольких уровней.

            Наконец, и в издательстве, и в Intranet должны быть авторы, создающие документы. Подчеркнем, что они не должны иметь прав на модификацию корпоративного дерева и отдельных документов. Их дело - передать свой труд редактору.

            Кроме официальных, корпоративных, в Intranet могут присутствовать групповые и личные документы, порядок работы с которыми (роли, права доступа) определяется, соответственно, групповыми и личными интересами.

            Переходя к вопросам поддержки жизненного цикла Intranet-информации, напомним о необходимости использования средств конфигурационного управления. Важное достоинство Intranet-технологии состоит в том, что основные операции конфигурационного управления - внесение изменений (создание новой версии) и извлечение старой версии документа - естественным образом вписываются в рамки Web-интерфейса. Те, для кого это необходимо, могут работать с деревом всех версий всех документов, подмножеством которого является дерево самых свежих версий.

***3.3.3. УПРАВЛЕНИЕ ДОСТУПОМ ПУТЕМ ФИЛЬТРАЦИИ ИНФОРМАЦИИ.***

            Мы переходим к рассмотрению мер программно-технического уровня, направленных на обеспечение информационной безопасности систем, построенных в технологии Intranet. На первое место среди таких мер мы поставим межсетевые экраны - средство разграничения доступа, служащее для защиты от внешних угроз и от угроз со стороны пользователей других сегментов корпоративных сетей.

            Отметим, что бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным.  Универсальная ОС - это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для получения нелегальных привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений (как и врач, не ведающий всех побочных воздействий рекомендуемых лекарств). Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.).

            Как указывалось выше, единственный перспективный путь связан с разработкой специализированных защитных средств, которые в силу своей простоты допускают формальную или неформальную верификацию. Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

            Межсетевой экран - это полупроницаемая мембрана, которая располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети) и контролирует все информационные потоки во внутреннюю сеть и из нее. Контроль информационных потоков состоит в их фильтрации, то есть в выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов политики безопасности организации.

*Рисунок 3.3.3.1*



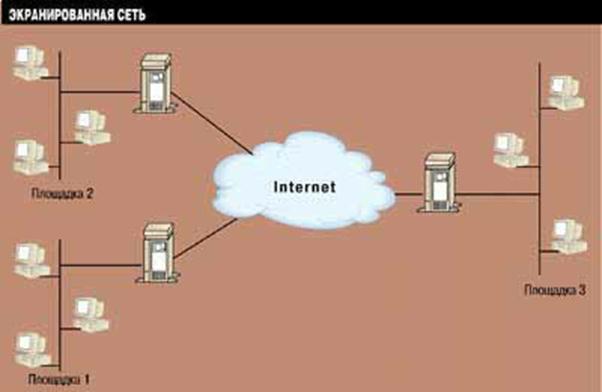
Межсетевой экран как средство контроля информационных потоков.

            Целесообразно разделить случаи, когда экран устанавливается на границе с внешней (обычно общедоступной) сетью или на границе между сегментами одной корпоративной сети. Соответственно, мы будет говорить о внешнем и внутреннем межсетевых экранах.

            Как правило, при общении с внешними сетями используется исключительно семейство протоколов TCP/IP. Поэтому внешний межсетевой экран должен учитывать специфику этих протоколов. Для внутренних экранов ситуация сложнее, здесь следует принимать во внимание помимо TCP/IP по крайней мере протоколы SPX/IPX, применяемые в сетях Novell NetWare. Иными словами, от внутренних экранов нередко требуется многопротокольность.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, является, скорее, исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования. В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний межсетевой экран является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

*Рисунок 3.3.3.2*



Экранирование корпоративной сети, состоящей из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования.

            При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. Межсетевые экраны также целесообразно классифицировать по тому, на каком уровне производится фильтрация - канальном, сетевом, транспортном или прикладном.  Соответственно, можно говорить об экранирующих концентраторах (уровень 2), маршрутизаторах (уровень 3), о транспортном экранировании (уровень 4) и о прикладных экранах (уровень 7). Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

            При принятии решения “пропустить/не пропустить”, межсетевые экраны могут использовать не только информацию, содержащуюся в фильтруемых потоках, но и данные, полученные из окружения, например текущее время.

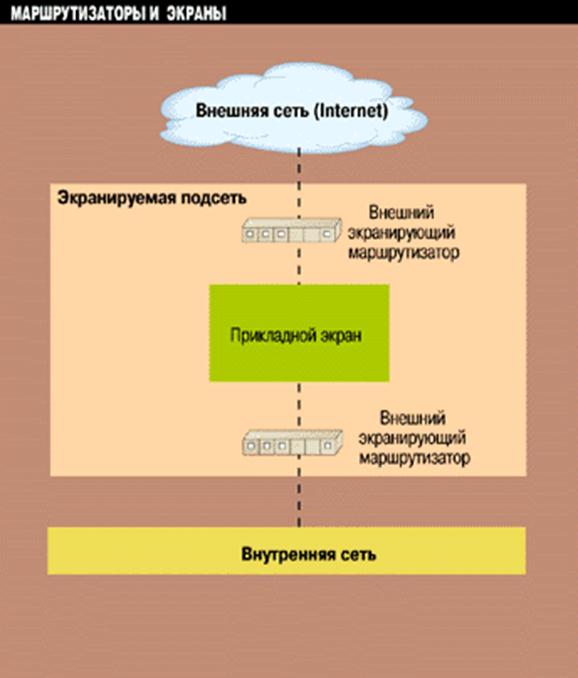
            Таким образом, возможности межсетевого экрана непосредственно определяются тем, какая информация может использоваться в правилах фильтрации и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует экран, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее экран может быть сконфигурирован. В то же время фильтрация на каждом из перечисленных выше уровней обладает своими достоинствами, такими как дешевизна, высокая эффективность или прозрачность для пользователей. В силу этой, а также некоторых других причин, в большинстве случаев используются смешанные конфигурации, в которых объединены разнотипные экраны. Наиболее типичным является сочетание экранирующих маршрутизаторов и прикладного экрана.

            Приведенная конфигурация называется экранирующей подсетью. Как правило, сервисы, которые организация предоставляет для внешнего применения (например “представительский” Web-сервер), целесообразно выносить как раз в экранирующую подсеть.

            Помимо выразительных возможностей и допустимого количества правил качество межсетевого экрана определяется еще двумя очень важными характеристиками - простотой применения и собственной защищенностью. В плане простоты использования первостепенное значение имеют наглядный интерфейс при задании правил фильтрации и возможность централизованного администрирования составных конфигураций. В свою очередь, в последнем аспекте хотелось бы выделить средства централизованной загрузки правил фильтрации и проверки набора правил на непротиворечивость. Важен и централизованный сбор и анализ регистрационной информации, а также получение сигналов о попытках выполнения действий, запрещенных политикой безопасности.

            Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. При выполнении централизованного администрирования следует еще позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность.

*Рисунок 3.3.3.3*



Сочетание экранирующих маршрутизаторов и прикладного экрана.

            Хотелось бы подчеркнуть, что природа экранирования (фильтрации), как механизма безопасности, очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Так, прикладной экран может осуществлять действия от имени субъектов внутренней сети, в результате чего из внешней сети кажется, что имеет место взаимодействие исключительно с межсетевым экраном. При таком подходе топология внутренней сети скрыта от внешних пользователей, поэтому задача злоумышленника существенно усложняется.

*Рисунок 3.3.3.4*



Истинные и кажущиеся информационные потоки.

            Более общим методом сокрытия информации о топологии защищаемой сети является трансляция “внутренних” сетевых адресов, которая попутно решает проблему расширения адресного пространства, выделенного организации.

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый видит лишь то, что ему положено.

Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, в частности таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация баз данных.

***3.3.4. БЕЗОПАСНОСТЬ ПРОГРАММНОЙ СРЕДЫ.***

            Идея сетей с так называемыми активными агентами, когда между компьютерами передаются не только пассивные, но и активные исполняемые данные (то есть программы), разумеется, не нова. Первоначально цель состояла в том, чтобы уменьшить сетевой трафик, выполняя основную часть обработки там, где располагаются данные (приближение программ к данным). На практике это означало перемещение программ на серверы. Классический пример реализации подобного подхода - это хранимые процедуры в реляционных СУБД.

Для Web-серверов аналогом хранимых процедур являются программы, обслуживающие общий шлюзовый интерфейс (Common Gateway Interface - CGI).

            CGI-процедуры располагаются на серверах и обычно используются для динамического порождения HTML-документов. Политика безопасности организации и процедурные меры должны определять, кто имеет право помещать на сервер CGI-процедуры. Жесткий контроль здесь необходим, поскольку выполнение сервером некорректной программы может привести к сколь угодно тяжелым последствиям. Разумная мера технического характера состоит в минимизации привилегий пользователя, от имени которого выполняется Web-сервер.

            В технологии Intranet, если заботиться о качестве и выразительной силе пользовательского интерфейса, возникает нужда в перемещении программ с Web-серверов на клиентские компьютеры - для создания анимации, выполнения семантического контроля при вводе данных и т.д. Вообще, активные агенты - неотъемлемая часть технологии Intranet.

            В каком бы направлении ни перемещались программы по сети, эти действия представляют повышенную опасность, т.к. программа, полученная из ненадежного источника, может содержать непреднамеренно внесенные ошибки или целенаправленно созданный зловредный код. Такая программа потенциально угрожает всем основным аспектам информационной безопасности:

•  доступности (программа может поглотить все наличные ресурсы);

•  целостности (программа может удалить или повредить данные);

•  конфиденциальности (программа может прочитать данные и передать их по сети).

***3.3.5. ЗАЩИТА WEB-СЕРВЕРОВ.***

            Наряду с обеспечением безопасности программной среды важнейшим будет вопрос о разграничении доступа к объектам Web-сервиса. Для решения этого вопроса необходимо уяснить, что является объектом, как идентифицируются субъекты и какая модель управления доступом - принудительная или произвольная - применяется.

            В Web-серверах объектами доступа выступают универсальные локаторы ресурсов (URL - Uniform (Universal) Resource Locator). За этими локаторами могут стоять различные сущности - HTML-файлы, CGI-процедуры и т.п.

Как правило, субъекты доступа идентифицируются по IP-адресам и/или именам компьютеров и областей управления. Кроме того, может использоваться парольная аутентификация пользователей или более сложные схемы, основанные на криптографических технологиях.

            В большинстве Web-серверов права разграничиваются с точностью до каталогов (директорий) с применением произвольного управления доступом. Могут предоставляться права на чтение HTML-файлов, выполнение CGI-процедур и т.д.

            Для раннего выявления попыток нелегального проникновения в Web-сервер важен регулярный анализ регистрационной информации.

            Разумеется, защита системы, на которой функционирует Web-сервер, должна следовать универсальным рекомендациям, главной из которых является максимальное упрощение. Все ненужные сервисы, файлы, устройства должны быть удалены. Число пользователей, имеющих прямой доступ к серверу, должно быть сведено к минимуму, а их привилегии - упорядочены в соответствии со служебными обязанностями.

            Еще один общий принцип состоит в том, чтобы минимизировать объем информации о сервере, которую могут получить пользователи. Многие серверы в случае обращения по имени каталога и отсутствия файла index.HTML в нем, выдают HTML-вариант оглавления каталога. В этом оглавлении могут встретиться имена файлов с исходными текстами CGI-процедур или с иной конфиденциальной информацией. Такого рода “дополнительные возможности” целесообразно отключать, поскольку лишнее знание (злоумышленника) умножает печали (владельца сервера).

***3.3.6. АУТЕНТИФИКАЦИЯ В ОТКРЫТЫХ СЕТЯХ.***

            Методы, применяемые в открытых сетях для подтверждения и проверки подлинности субъектов, должны быть устойчивы к пассивному и активному прослушиванию сети. Суть их сводится к следующему.

•  Субъект демонстрирует знание секретного ключа, при этом ключ либо вообще не передается по сети, либо передается в зашифрованном виде.

• Субъект демонстрирует обладание программным или аппаратным средством генерации одноразовых паролей или средством, работающим в режиме “запрос-ответ”. Нетрудно заметить, что перехват и последующее воспроизведение одноразового пароля или ответа на запрос ничего не дает злоумышленнику.

• Субъект демонстрирует подлинность своего местоположения, при этом используется система навигационных спутников.

***3.3.7. ПРОСТОТА И ОДНОРОДНОСТЬ АРХИТЕКТУРЫ.***

            Важнейшим аспектом информационной безопасности является управляемость системы. Управляемость - это и поддержание высокой доступности системы за счет раннего выявления и ликвидации проблем, и возможность изменения аппаратной и программной конфигурации в соответствии с изменившимися условиями или потребностями, и оповещение о попытках нарушения информационной безопасности практически в реальном времени, и снижение числа ошибок администрирования, и многое, многое другое.

            Наиболее остро проблема управляемости встает на клиентских рабочих местах и на стыке клиентской и серверной частей информационной системы. Причина проста - клиентских мест гораздо больше, чем серверных, они, как правило, разбросаны по значительно большей площади, их используют люди с разной квалификацией и привычками. Обслуживание и администрирование клиентских рабочих мест - занятие чрезвычайно сложное, дорогое и чреватое ошибками.  Технология Intranet за счет простоты и однородности архитектуры позволяет сделать стоимость администрирования клиентского рабочего места практически нулевой. Важно и то, что замена и повторный ввод в эксплуатацию клиентского компьютера могут быть осуществлены очень быстро, поскольку это “клиенты без состояния”, у них нет ничего, что требовало бы длительного восстановления или конфигурирования.

            На стыке клиентской и серверной частей Intranet-системы находится Web-сервер. Это позволяет иметь единый механизм регистрации пользователей и наделения их правами доступа с последующим централизованным администрированием. Взаимодействие с многочисленными разнородными сервисами оказывается скрытым не только от пользователей, но и в значительной степени от системного администратора.

            Задача обеспечения информационной безопасности в Intranet оказывается более простой, чем в случае произвольных распределенных систем, построенных в архитектуре клиент/сервер. Причина тому - однородность и простота архитектуры Intranet. Если разработчики прикладных систем сумеют в полной мере воспользоваться этим преимуществом, то на программно-техническом уровне им будет достаточно нескольких недорогих и простых в освоении продуктов. Правда, к этому необходимо присовокупить продуманную политику безопасности и целостный набор мер процедурного уровня.

**3.4. PGP.**

   Алгоритмы шифрования реализуются программными или аппаратными средствами. Есть великое множество чисто программных реализаций различных алгоритмов. Из-за своей дешевизны (некoторые и вовсе бесплатны), а также все большего быстродействия процессоров ПЭВМ, простоты работы и безотказности они весьма конкурентоспособны.

   Нельзя не упомянуть пакет PGP (Pretty Good Privacy, автор Philip Zimmermann), в котором комплексно решены практически все проблемы защиты передаваемой информации. Применены сжатие данных перед шифрованием, мощное управление ключами, вычисление контрольной функции для цифровой подписи, надежная генерация ключей.

В Internet фактическим стандартом шифрования является программа PGP (Pretty Good Privacy), разработанная в 1991 году Филиппом Циммерманом. PGP позволяет зашифровывать сообщения так, чтобы только получатели могли их прочесть, или ставить на них цифровые подписи так, чтобы можно было убедиться в подлинности автора. В настоящий момент программа доступна на платформах UNIX, DOS, Macintosh и VAX. PGP свободно распространяется по Internet для некоммерческих пользователей вместе с 75-страничным справочным руководством. Кроме того, последняя версия PGP 2.6.6 можно приобрести в MIT.

PGP работает следующим образом. У каждого пользователя имеется два ключа: секретный ключ и открытый ключ. Секретный ключ он оставляет в тайне, а открытый сообщает всем своим приятелям. При помощи каждого из ключей можно прочитать сообщение, зашифрованное при помощи другого. Если ваши коллеги хотят послать вам конфиденциальное сообщение, они могут воспользоваться вашим открытым PGP-ключом; при помощи секретного ключа оно может быть расшифровано. Если же вы хотите поставить цифровую подпись, в этом вам поможет секретный ключ; при этом у получателя обязательно должен быть экземпляр открытого ключа.

PGP предназначена, в первую очередь, для защиты электронной почты, хотя ее целиком можно использовать и для защиты файлов на жестком диске. Особенно привлекательными чертами PGP есть многочисленные plug-ins для популярных почтовых программ, таких как Eudora, Netscape и Outlook. Plug-ins настраивают  PGP для этих программ и дополняют их некоторыми приятными мелочами, такими, как дополнительная кнопка панели инструментов. Иконка в правом нижнем углу (tray), всплывающая панель инструментов (floating toolbox) и меню правой клавиши мышки (right-click menu) в PGP необычайно логично и удобно продуманы. Поэтому она очень проста в управлении.

Как только вы создали свои ключи для шифрования, можете соединиться с одним из PGP-серверов и разместить в нем свой открытый ключ. С этого момента каждый, кто хочет, может послать вам электронную почту в зашифрованном виде. Если вы используете преимущественно одну и ту же почтовую программу, шифрование и дешифрование будет не сложнее простого нажатия кнопки. Если же вы используете разные программы, достаточно будет забрать письмо в буфер и дать команду шифровать в буфере. После этого можно вернуть письмо в почтовую программу и отослать.

PGP особенно быстродейственна при пересылке зашифрованной информации пользователям Mac. Опция Smart Binary новых версий облегчает пересылку зашифрованных писем из Mac на Windows (и в обратном направлении).

Можно столкнуться с системой защиты PGP в программе, которая называется Nuts & Bolts, производство Helix Software. Это та же программа, только PGP – более новая версия. Network Associates поглотила Helix и завладела правами на продукт. Новая версия PGP for Personal Privacy – совместима с предыдущими версиями, в том числе Nuts & Bolts. В целом Pretty Good Privacy – это приятная и удобная в работе программа.



Основные команды PGP

**pgp –kg**                  Создать два ключа и вашу связку отрытых ключей.

**Pgp –kx [a]** *имя\_пользователя*        Извлечь ключ (например, ваш открытый ключ)

 из связки ключей, чтобы передать его кому-нибудь еще.

**Pgp –ka** *имя\_файла*              Добавить чей-либо ключ в связку.

**Pgp –e** *имя\_файла получатель/получатели*   Зашифровать файл так, чтобы только определенные

 пользователи могли его прочитать (для этого необходимо иметь копию

 соответствующих отрытых ключей).

**Pgp –es** *имя\_файла получатель/получатели*   Зашифровать файл и поставить цифровую подпись.

**Pgp –s** *имя\_файла*              Поставить цифровую подпись.

 (Создается двоичный файл, который не так просто переслать по почте;

 получателям необходимо воспользоваться PGP).

**Pgp –sa** *имя\_файла*              Поставить цифровую подпись и сохранить

 результат как ASCII-текст. (Просто пересылается по сети, но также требует PGP для прочтения).

**Pgp** *зашифрованный\_файл*           Проверить подпись на зашифрованном файле.

**Pgp** *зашифрованный\_файл расшифрованный\_файл* Расшифровать присланный файл.

**3.5. Blowfish.**

Blowfish 97 использует ряд схем систем защиты в два этапа. Первичный механизм шифрования базируется на Blowfish, которую разработал в 1993 году Bruce Schneier. Blowfish – это симметричный шифр, который использует ключи сменной длины – от 32 бит до 448 бит. Система защиты Blowfish не запатентована, и, следовательно, разрешена для использования в любом продукте, в который входит. Существуют четыре разных варианта Blowfish, вы часто можете встретиться с ней среди опций многих программ защиты.

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">

Blowfish -блочный шифр с ключом переменной длины. Это подходит для приложений, где ключ изменяется не часто, подобных линии связи или автоматическому шифрователю файла. Он значительно быстрее, чем DES при выполнении на 32-битных процессорах с большим КЭШем данных, таких как Pentium и PowerPC.

**ОПИСАНИЕ АЛГОРИТМА**

Blowfish - 64-битный блочный шифр с ключом переменной длины. Алгоритм включает в себя 2 части: часть расширения ключей и часть шифрования данных. Расширение ключа преобразует ключ, в большинстве 448-битный, в несколько суммированных массивов подключей в 4168 байт.

Шифрование данных происходит через 16-итерационную сеть Feistel. Каждая итерация состоит из ключе-зависимой перестановки, и зависящей от ключа и данных замены. Все операции - XOR и сложение на 32-битных словах. Единственные дополнительные операции - 4 поиска в индексированных массивах на итерацию.

Подключи: Blowfish использует большое количество подключей. Эти ключи должны быть предварительно вычислены перед любым шифрованием данных или расшифровкой.

1. P-массив включает 18 32-битных подключей:   
P1, P2,..., P18.

2.Имеются четыре 32-битных S-блока с 256 входами каждый:   
S1,0, S1,1,..., S1,255;   
S2,0, S2,1,..,, S2,255;   
S3,0, S3,1,..., S3,255;   
S4,0, S4,1,..,, S4,255.

Шифрование: Blowfish - сеть Feistel, которая включает 16 итераций.

Реализации Blowfish, которые требуют наибольших скоростей, не должны организовываться в цикле, что гарантирует присутствие всех подключей в КЭШе.

Всего, 521 итерация требуются, для генерации всех требуемых подключей. Прикладные программы могут сохранить подключи, чтобы сократить время.

**MINI-BLOWFISH**

Следующие малые версии Blowfish определены исключительно для криптоанализа. Они не предлагаются для реализации. Blowfish-32 имеет размер блока в 32 бита, и массивы подключей с 16 битными входами (каждый S-блок имеет 16 входов). Blowfish-16 имеет размер блока в 16-бит, и массивы подключей с 8-битными входами (каждый S-блок имеет 4 входа).

**РЕАЛИЗАЦИЯ ПРОЕКТА**

Вероятность ошибок в реализации алгоритма мала, т.к. сами S блоки и P-блок очень просты. 64-битный блок в действительности разбивается на 32-битные слова, что совместимо с существующими алгоритмами. В Blowfish можно легко повышать размер блока до 128-бит, и понижать размер блока. Криптоанализ вариантов мини-Blowfish может быть значительно проще, чем криптоанализ полной версии.

Сеть Feistel, составляющая тело Blowfish, разработана так, чтобы при наибольшей простоте она сохраняла свои криптографические свойства.

В проекте алгоритма существует два способа гарантировать, что ключ является достаточно длинным, чтобы достичь нужного уровня защиты. Первый в том, чтобы тщательно разработать алгоритм так, чтобы энтропия случайно введенного ключа сохранялась, так как тогда не существует другого метода криптоанализа, кроме атаки в "лоб". Другой способ - в увеличении длины ключа настолько, что уменьшение эффективности ключа на несколько битов не дает больших преимуществ. Так как Blowfish разработан для больших процессоров с большим размером памяти я выбрал последний способ.

Отнимающий много времени процесс порождения подключей добавляет сложность для нападения "в лоб". Всего 522 итераций алгоритма шифрования требуется, чтобы проверить один ключ, что добавляет 29 шагов при любом нападение в лоб.

**ВОЗМОЖНЫЕ УПРОЩЕНИЯ**

Меньшее количество итераций. Вероятно, возможно уменьшение количества итераций с 16 до 8 без сильного ослабления защиты. Число итераций требуемых для защиты может зависеть от длины ключа. Обратите внимание, что с имеющейся процедурой порождения подключа, алгоритм с 8 итерациями не может обрабатывать ключ длиной больше 192 бит.

Непрерывное вычисление подключа. Текущий метод вычисления подключей требует, чтобы все подключи вычислялись перед любым шифрованием. Фактически невозможно вычислить последний подключ последнего S-блока без вычисления перед этим предыдущего ключа. Был бы предпочтительней альтернативный метод вычисления подключа: когда каждый подключ может быть вычислен независимо от другого подключа. Высококачественные реализации могли бы предварительно вычислять подключи для более высокой скорости, но реализации с низкими требованиями могут вычислять подключи, когда это необходимо.

Наиболее эффективный способ взломать Blowfish - через полный перебор ключей Исходный текст на Си и тестовые векторы может получить любой, желающий реализовать алгоритм, в соответствие с законами США об экспорте.

Blowfish незапатентован, и будет таким оставаться во всех странах. Алгоритм тем самым помещен в общую область и может быть использован любым.

Blowfish - это простая и легкая в понимании программа. Панель инструментов содержит только картинки и ни одного слова. Четкая система подсказок. Выбрав файл, и нажав на изображение «замка», вы получите сообщение, что сейчас возможно использование шифрования только с ключом из пяти позиций, но после регистрации доступными будут и 32000-символьные ключи шифрования. После введения ключа процесс шифрования длится несколько секунд. Файл получает новое расширение (.BFA), которое служит командой для операционной системы при встрече с ним запустить в действие Blowfish Advanced.

В сети существует также защитная программа под Windows 95/NT, которая использует механизм Blowfish. EncLib 5/5 Использует для шифрования варианты Blowfish CDC и ECB.

**3.6.KERBEROS.**

Развитие криптологии с открытым ключом позволило криптологическим системам довольно быстро найти широкое коммерческое применение. Но интенсивное использование криптографии не обходится без “накладок”. Время от времени появляется информация о неприятностях в той или иной системе защиты. Последним нашумевшим в мире происшествием стал взлом системы Kerberos. Система эта, разработанная в середине 80-х годов, довольно популярна в мире, и ее взлом вызвал немалое беспокойство пользователей.

Проблема защиты компьютерных сетей от несанкционированного доступа приобрела особую остроту. Развитие коммуникационных технологий позволяет строить сети распределенной архитектуры, объединяющие большое количество сегментов, расположенных на значительном удалении друг от друга. Все это вызывает увеличение числа узлов сетей, разбросанных по всему миру, и количества различных линий связи между ними, что, в свою очередь, повышает риск несанкционированного подключения к сети для доступа к важной информации. Особенно неприятной такая перспектива может оказаться для банковских или государственных структур, обладающих секретной информацией коммерческого или любого другого характера. В этом случае необходимы специальные средства идентификации пользователей в сети, обеспечивающие доступ к информации лишь в случае полной уверенности в наличии у пользователя прав доступа к ней. Существует ряд разработок, позволяющих с высокой степенью надежности идентифицировать пользователя при входе в систему. Среди них, например, есть технологии, идентифицирующие пользователя по сетчатке глаза или отпечаткам пальцев. Кроме того, ряд систем использует технологии, основанные на применении специального идентификационного кода, постоянно передаваемого по сети. Так, при использовании устройства (фирмы Security Dinamics) обеспечивается дополнительная информация о пользователе в виде шестизначного кода. В данном случае работа в сети невозможна без наличия специальной карты SecureID (похожей на кредитную), которая обеспечивает синхронизацию изменяющегося кода пользователя с хранящимися на UNIX-хосте. При этом доступ в сеть и работа в ней может осуществляться лишь при знании текущего значения кода, который отображается на дисплее устройства SecureID. Однако основным недостатком этой и ей подобных систем является необходимость в специальном оборудовании, что вызывает неудобства в работе и дополнительные затраты. Система Kerberos (по-русски – Цербер), разработанная участниками проекта Athena, обеспечивает защиту сети от несанкционированного доступа, базируясь исключительно на программных решениях, и предполагает многократное шифрование передаваемой по сети управляющей информации. Kerberos обеспечивает идентификацию пользователей сети и серверов, не основываясь на сетевых адресах и особенностях операционных систем рабочих станций пользователей, не требуя физической защиты информации на всех машинах сети и исходя из предположения, что пакеты в сети могут быть легко прочитаны и при желании изменены.

*Клиент/Kerberos/Сервер*.

Kerberos имеет структуру типа клиент/сервер и состоит из клиентских частей, установленных на все машины сети (рабочие станции пользователей и серверы), и Kerberos-сервера (или серверов), располагающегося на каком-либо (не обязательно выделенном) компьютере.Kerberos-сервер, в свою очередь, делится на две равноправные части: сервер идентификации (authentication server) и сервер выдачи разрешений (ticket granting server). Следует отметить, что существует и третий сервер Kerberos, который, однако, не участвует в идентификации пользователей, а предназначен для административных целей. Область действия Kerberos (realm) распространяется на тот участок сети, все пользователи которого зарегистрированы под своими именами и паролями в базе Kerberos-сервера и где все серверы обладают общим кодовым ключом с идентификационной частью Kerberos. Эта область не обязательно должна быть участком локальной сети, поскольку Kerberos не накладывает ограничения на тип используемых коммуникаций. Упрощенно модель работы Kerberos можно описать следующим образом. Пользователь  (Kerberos-клиент), желая получить доступ к ресурсу сети, направляет запрос идентификационному серверу Kerberos. Последний идентифицирует пользователя с помощью его имени и пароля и выдает разрешение на доступ к серверу выдачи разрешений, который, в свою очередь, дает “добро” на использование необходимых ресурсов сети. Однако данная модель не отвечает на вопрос о надежности защиты информации, поскольку, с одной стороны, пользователь не может посылать идентификационному серверу свой пароль по сети, а с другой – разрешение на доступ к обслуживанию в сети не может быть  послано пользователю в виде обычного сообщения. В обоих случаях информация может быть перехвачена и использована для несанкционированного доступа в сеть. Для того, чтобы избежать подобных неприятностей Kerberos применяет сложную систему многократного шифрования при передаче любой управляющей информации в сети. Доступ пользователей к сетевым серверам, файлам, приложениям, принтерам и т.д. осуществляется по следующей схеме. Клиент (под которым в дальнейшем будет пониматься клиентская часть Kerberos, установленная на рабочей станции пользователя) направляет запрос идентификационному серверу на выдачу “разрешения на получение разрешения” (ticket-granting ticket), которое даст возможность обратиться к серверу выдачи разрешений. Идентификационный сервер адресуется к базе данных, хранящей информацию о всех пользователях, и на основании содержащегося в запросе имени пользователя определяет его пароль. Затем клиенту отсылается “разрешение на получение разрешения” и специальный код сеанса (session key), которые шифруются с помощью пароля пользователя как ключа. При получении этой информации пользователь на его рабочей станции должен ввести свой пароль, и если он совпадает с хранящимися в базе Kerberos-сервера, “разрешение на получение разрешения” и код сеанса будут успешно расшифрованы. Таким образом решается проблема с защитой пароля – в данном случае он не передается по сети. После того как клиент зарегистрировался с помощью идентификационного сервера Kerberos, он отправляет запрос серверу выдачи разрешений на получение доступа к требуемым ресурсам сети. Этот запрос (или “разрешение на получение разрешения”) содержит имя пользователя, его сетевой адрес, отметку времени, срок жизни этого разрешения и код сеанса.“Разрешение на получение разрешения” зашифровывается два раза: сначала с помощью специального кода, который известен только идентификационному серверу и серверу выдачи разрешений, а затем, как уже было сказано, с помощью пароля пользователя. Это предотвращает не только возможность использования этого разрешения при его перехвате, но и делает его недоступным самому пользователю. Для того чтобы сервер выдачи разрешений дал клиенту доступ к требуемым ресурсам, недостаточно только “разрешения на получение разрешения”. Вместе с ним клиент посылает так называемый аутентикатор (authenticator), зашифровываемый с помощью кода сеанса и содержащий имя пользователя, его сетевой адрес и еще одну отметку времени. Сервер выдачи разрешений расшифровывает полученное от клиента “разрешение на получение разрешения”, проверяет, не истек ли срок его “годности”, а затем сравнивает имя пользователя и его сетевой адрес, находящиеся в разрешении, с данными, которые указаны в заголовке пакета пришедшего сообщения. Однако на этом проверки не заканчиваются. Сервер выдачи разрешений расшифровывает аутентикатор с помощью кода сеанса и еще раз сравнивает имя пользователя и его сетевой адрес с предыдущими двумя значениями, и только в случае положительного результата может быть уверен наконец, что клиент именно тот, за кого себя выдает. Поскольку аутентикатор используется для идентификации клиента всего один раз и только в течение определенного периода времени, становится практически невозможным одновременный перехват “разрешения на получение разрешения” и аутентикатора для последующих попыток несанкционированного доступа к ресурсам сети. Каждый раз, при необходимости доступа к серверу сети, клиент посылает “разрешение на получение разрешения” многоразового использования и новый аутентикатор. После успешной идентификации клиента в качестве источника запроса сервер выдачи разрешений отсылает пользователю разрешение на доступ к ресурсам сети (которое может использоваться многократно в течение некоторого периода времени) и новый код сеанса. Это разрешение зашифровано с помощью кода, известного только серверу выдачи разрешений и серверу, к которому требует доступа клиент, и содержит внутри себя копию нового кода сеанса. Все сообщение (разрешение и новый код сеанса)  зашифровано с помощью старого кода сеанса, поэтому расшифровать его может только клиент. После расшифровки клиент посылает целевому серверу, ресурсы которого нужны пользователю, разрешение на доступ и аутентикатор, зашифрованные с помощью нового кода сеанса. Для обеспечения еще более высокого уровня защиты, клиент, в свою очередь, может потребовать идентификации целевого сервера, чтобы обезопаситься от возможного перехвата информации, дающей право на доступ к ресурсам сети. В этом случае он требует от сервера высылки значения отметки времени, увеличенного на единицу и зашифрованного с помощью кода сеанса. Сервер извлекает копию кода сеанса, хранящуюся внутри разрешения на доступ к серверу, использует его для расшифровки аутентикатора, прибавляет к отметке времени единицу, зашифровывает полученную информацию с помощью кода сеанса и отсылает ее клиенту. Расшифровка этого сообщения позволяет клиенту идентифицировать сервер. Использование в качестве кода отметки времени обеспечивает уверенность в том, что пришедший клиенту ответ от сервера не является повтором ответа на какой-либо предыдущий запрос. Теперь клиент и сервер готовы к передаче необходимой информации с должной степенью защиты. Клиент обращается с запросами к целевому серверу, используя полученное разрешение. Последующие сообщения зашифровываются с помощью кода сеанса. Более сложной является ситуация, когда клиенту необходимо дать серверу право пользоваться какими-либо ресурсами от его имени. В качестве примера можно привести ситуацию, когда клиент посылает запрос серверу печати, которому затем необходимо получить доступ к файлам пользователя, расположенным на файл-сервере. Кроме того, при входе в удаленную систему пользователю необходимо, чтобы все идентификационные процедуры выполнялись так же, как и с локальной машины. Эта проблема решается установкой специальных флагов в “разрешении на получение разрешения” (дающих одноразовое разрешение на доступ к серверу от имени клиента для первого примера и обеспечивающих постоянную работу в этом режиме для второго). Поскольку, как было сказано выше, разрешения строго привязаны к сетевому адресу обладающей ими станции, то при наличии подобных флагов сервер выдачи разрешений должен указать в разрешении сетевой адрес того сервера, которому передаются полномочия на действия от имени клиента. Следует отметить также, что для всех описанных выше процедур идентификации необходимо обеспечить доступ к базе данных Kerberos только для чтения. Но иногда требуется изменять базу, например, в случае изменения ключей или добавления новых пользователей. Тогда используется третий сервер Kerberos – административный (Kerberos Administration Server). Не вдаваясь в подробности его работы, следует отметить, что его реализации могут сильно отличаться (так, возможно ведение нескольких копий базы одновременно).

*Связь между Kerberos–областями*.

Как уже было сказано выше, при использовании Kerberos–серверов сеть делится на области действия Kerberos. Схема доступа клиента, находящегося в области действия одного Kerberos–сервера, к ресурсам сети, расположенным в области действия другого Kerberos, осуществляется следующим образом. Оба Kerberos-сервера должны быть обоюдно зарегистрированы, то есть знать общие секретные ключи и, следовательно, иметь доступ к базам пользователей друг друга. Обмен этими ключами между Kerberos–серверами (для работы в каждом направлении используется свой ключ) позволяет зарегистрировать сервер выдачи разрешений каждой области как клиента в другой области. После этого клиент, требующий доступа к ресурсам, находящимся в области действия другого Kerberos–сервера, может получить разрешение от сервера выдачи разрешений своего Kerberos по описанному выше алгоритму. Это разрешение, в свою очередь, дает право доступа к серверу выдачи разрешений другого Kerberos–сервера и содержит в себе отметку о том, в какой Kerberos–области зарегистрирован пользователь. Удаленный сервер выдачи разрешений использует один из общих секретных ключей для расшифровки этого разрешения (который, естественно, отличается от ключа, используемого в пределах этой области) и при успешной расшифровке может быть уверен, что разрешение выдано клиенту соответствующей Kerberos–области. Полученное разрешение на доступ к ресурсам сети предъявляется целевому серверу для получения соответствующих услуг. Следует, однако, учитывать, что большое число Kerberos–серверов в сети ведет к увеличению количества передаваемой идентификационной информации при связи между разными Kerberos–областями. При этом увеличивается нагрузка на сеть и на сами Kerberos–серверы. Поэтому более эффективным следует считать наличие в большой сети всего нескольких Kerberos–серверов с большими областями действия, нежели использование множества Kerberos–серверов. Так, Kerberos-система, установленная компанией Digital Equipment для большой банковской сети, объединяющей отделения в Нью-Йорке, Париже и Риме, имеет всего один Kerberos–сервер. При этом, несмотря на наличие в сети глобальных коммуникаций, работа Kerberos–системы практически не отразилась на производительности сети.

***Kerberos-5.***

К настоящему времени Kerberos выдержал уже четыре модификации, из которых четвертая получила наибольшее распространение. Недавно группа, продолжающая работу над  Kerberos, опубликовала спецификацию пятой версии системы, основные особенности которой отражены в стандарте RFC 1510. Эта модификация Kerberos имеет ряд новых свойств, из которых можно выделить следующие. Уже рассмотренный ранее механизм передачи полномочий серверу на действия от имени клиента, значительно облегчающий идентификацию в сети в ряде сложных случаев, является нововведением пятой версии. Пятая версия обеспечивает более упрощенную идентификацию пользователей в удаленных Kerberos-областях, с сокращенным числом передач секретных ключей между этими областями. Данное свойство, в свою очередь, базируется на механизме передачи полномочий. Если в предыдущих версиях Kerberos для шифрования использовался исключительно алгоритм DES (Data Encryption Standard – Стандарт Шифрования Данных), надежность которого вызывала некоторые сомнения, то вданной версии возможно использование различных алгоритмов шифрования, отличных от DES.

***Заключение.***

Многие производители сетевого и телекоммуникационного оборудования обеспечивают поддержку работы с Kerberos в своих устройствах. Так, фирма TELEBIT, являясь крупнейшим поставщиком маршрутизаторов для связи по коммутируемым и выделенным линиям, недавно анонсировала поддержку Kerberos–клиента семейством маршрутизаторов NetBlazer. Снабженные UNIX–подобной операционной системой, устройства NetBlazer обеспечивают их удаленное конфигурирование по сети с помощью функций telnet и rlogin .Поэтому работоспособность сети, в особенности если это сеть достаточно больших размеров, сильно зависит от защищенности коммуникационных узлов, которыми являются маршрутизаторы NetBlazer, от непредвиденных или злонамеренных изменений конфигурации. Использование Kerberos в таких сетях позволит обеспечить доступ к внутренним установкам маршрутизатора только администраторам сети. Следует, однако, отметить, что использование Kerberos не является решением всех проблем, связанных с попытками несанкционированного доступа в сеть (например, он бессилен, если кто-либо узнал пароль пользователя), поэтому его наличие не исключает других стандартных средств поддержания соответствующего уровня секретности в сети. Несмотря на это, Kerberos в настоящее время является одним из наиболее известных способов защиты сети от несанкционированного доступа. Основываясь исключительно на программных средствах и не требуя дополнительных “железных” устройств, он обеспечивает защиту сети с минимальным воздействием на трафик. Kerberos обеспечивает такой уровень защиты сети, при котором подключение к ней не дает возможности доступа к важной информации без регистрации пользователя в секретной базе Kerberos (что может быть проделано только с участием администратора сети). При этом для пользователя сети такая защита практически прозрачна, поскольку требует от него лишь дополнительного ввода пароля.

В случае с Kerberos неприятность  заключалась не в алгоритме шифрования, а в способе получения случайных чисел, т.е. в методе реализации алгоритма. Когда в октябре прошлого года пришло известие о просчетах в системе генерации случайных чисел в программных продуктах Netscape, обнаруженных студентами университета Беркли, Стивен Лодин обнаружил подобную неприятность с Kerberos. Совместно с Брайаном Доулом он сумел найти брешь и в системе Kerberos. Действующие лица этой истории – не дилетанты. Выпускники университета Purdue (штат Иллинойс) сотрудничали с лабораторией COAST (Computer Operations, Audit and Security Technology), профессионально занятой вопросами компьютерной безопасности и руководимой проф. Спаффордом, который является также основателем PCERT (Purdue Computer Emergency Response Team) – университетского отряда “быстрого реагирования” на компьютерные ЧП. PCERT, в свою очередь, член аналогичной международной организации FIRST (Forum of Incident Response Team).

Характерно содержание первого обращения к прессе (от 16 февраля 1996 г.), которое от лица первооткрывателей сделал проф. Спаффорд. В нем, наряду с информацией о ненадежности системы паролей и возможностях ее взлома в течение пяти минут, говорится о задержке дальнейшего распространения технической информации до тех пор, пока разработчиками не будут внесены коррективы препятствующие несанкционированному доступу.

4. Виртуальные частные сети.

Одной из важнейших задач является защита потоков корпоративных данных, передаваемых по открытым сетям. Открытые каналы могут быть надежно защищены лишь одним методом – криптографическим.

Так называемые выделенные линии не обладают особыми преимуществами перед линиями общего пользования в плане информационной безопасности. Выделенные линии хотя бы частично будут располагаться в неконтролируемой зоне, где их могут повредить или осуществить к ним несанкционированное подключение. Единственное реальное достоинство – это гарантированная пропускная способность выделенных линий, а вовсе не какая-то повышенная защищенность. Впрочем, современные оптоволоконные каналы способны удовлетворить потребности многих абонентов, поэтому и указанное достоинство не всегда облечено в реальную форму.

Любопытно упомянуть, что в мирное время 95 % трафика Министерства обороны США передается через сети общего пользования (в частности через). В военное время эта доля должна составлять «лишь» 70 %. Можно предположить, что Пентагон – не самая бедная организация. Американские военные полагаются на сети общего пользования потому, что развивать собственную инфраструктуру в условиях быстрых технологических изменений – занятие очень дорогое и бесперспективное, оправданное даже для критически важных национальных организаций  только в исключительных случаях.

Представляется естественным возложить на межсетевой экран задачу шифрования и дешифрования корпоративного трафика на пути во внешнюю сеть и из нее. Чтобы такое шифрование/дешифрование стало возможным, должно произойти начальное распределение ключей. Современные криптографические технологии предлагают для этого целый ряд методов.

После того, как межсетевые экраны осуществили криптографическое закрытие корпоративных потоков данных, территориальная разнесенность сегментов сети проявляется лишь в разной скорости обмена с разными сегментами. В остальном вся сеть выглядит как единое целое, а от абонентов не требуется привлечение каких-либо дополнительных защитных средств.

 Пожалуй, нигде слово виртуальный не получило столь широкого распространения, как в сфере информационных технологий: виртуальная память, виртуальная машина, виртуальная реальность, виртуальный канал, виртуальный офис. Это произошло благодаря возможности так запрограммировать логику функционирования объекта, что для пользователя его (логические) поведение и свойства никак не будут отличаться от реального прототипа. Бегство в «виртуальный мир» может быть вызвано, скажем, принципиальной невозможностью оперировать с реальным объектом, экономическими соображениями либо временным фактором.

Виртуальные частные сети (Virtual Private Networks - VPN) являются не только «горячей» темой для индустриальных аналитиков, но привлекают также пристальное внимание как провайдеров сетевых услуг (Network Service Provider - NSP) и Internet-провайдеров (ISP), так и корпоративных пользователей. Компания Infonetics Research прогнозирует, что рынок VPN будет расти более чем на 100 % ежегодно вплоть до 2001 г., и его объем достигнет 12 млрд. долл. Она также сообщает, что 92 % крупных Internet-провайдеров и 60 % от общего числа ISP планируют предоставлять услуги VPN к концу 1998 г.

Прежде чем переходить к анализу причин, вызвавших столь бурный рост популярности VPN, напомним, что просто частные (корпоративные) сети передачи данных строятся, как правило, с использованием арендованных (выделенных) каналов связи коммутируемых телефонных сетей общего пользования (Public Switched Telephone Network - PSTN).  В течение многих лет такие частные сети проектировались с учетом конкретных корпоративных требований, что в результате транслировалось в фирменные протоколы, поддерживающие фирменные же приложения (правда, в последнее время приобрели популярность протоколы Frame Relay и ATM). Выделенные каналы позволяют обеспечить надежную защиту конфиденциальной информации, однако оборотная сторона медали – это высокая стоимость эксплуатации и трудности при расширении сети, не говоря уже о возможности подключения к ней мобильного пользователя в непредусмотренной точке. В то же время для современного бизнеса характерны значительное рассредоточение и мобильность рабочей силы. Все больше пользователей нуждается в доступе к корпоративной информации посредством коммутируемых каналов, увеличивается также количество сотрудников, работающих на дому. Западные аналитики предсказывают, что к концу 1999 г. 80 % корпоративных пользователей будут иметь, по крайней мере, по одному портативному компьютеру (безусловно, проекция этого предсказания на Украину может вызвать только улыбку, но рано или поздно украинская экономика, изнасилованная прогрессом, вынуждена будет принять правила игры, диктуемые промышленно развитыми странами).

Далее, частные сети не в состоянии обеспечить такие же возможности для коммерческой деятельности, которые предоставляет Internet и IP-базированные приложения, к примеру, продвижение продукции, поддержка заказчиков или постоянная связь с поставщиками. Такое взаимодействие в режиме on-line требует объединения частных сетей, которые, как правило, используют разные протоколы и приложения, разные системы управления сетью и разных поставщиков услуг связи.

Таким образом, высокая стоимость, статичность и трудности, возникающие при необходимости объединить частные сети, базирующиеся на разных технологиях, вступают в противоречие с динамически развивающимся бизнесом, его стремлением к децентрализации и проявляющейся в последнее время тенденцией к слиянию компаний.

В то же время параллельно существуют лишенные этих  недостатков сети передачи данных общего пользования и Internet, буквально окутавшая своей «паутиной» весь земной шар. Правда, они лишены и наиболее важного достоинства частных сетей – надежной защиты корпоративной информации. Технология виртуальных частных сетей и позволяет объединить гибкость, масштабируемость, низкую стоимость и доступность буквально в режиме «anytime anywhere»  Internet и сетей  общего пользования с безопасностью, характерной для частных сетей. По своей сути VPN являются частными сетями, которые для передачи трафика используют глобальные сети общего доступа (Internet, Frame Relay, ATM). Виртуальность же проявляется в том, что для корпоративного пользователя они представляются выделенными частными сетями. Рассмотрим основные требования, которые предъявляются к виртуальным частным сетям.

**4.1. СОВМЕСТИМОСТЬ.**

Проблемы совместимости не возникают, если VPN прямо используют службы Frame Relay и ATM, поскольку они довольно хорошо приспособлены для работы в мультипротокольной среде и пригодны как для IP-, так и для не IP–приложений. Все, что требуется в этом случае, так это наличие соответствующей сетевой инфраструктуры, покрывающей необходимый географический район. В качестве устройств доступа чаще всего используются Frame Relay Access Device (FRAD) или маршрутизаторы с интерфейсами Frame Relay и ATM. Многочисленные постоянные или коммутируемые виртуальные каналы могут работать (виртуально) с любой смесью протоколов и топологий. Дело осложняется, если VPN базируется на Internet. В этом случае требуется, чтобы приложения были совместимы с IP–протоколом. При условии выполнения этого требования для построения VPN можно использовать Internet «как она есть», предварительно обеспечив необходимый уровень безопасности. Но поскольку большинство частных сетей являются мультипротокольными или используют неофициальные, внутренние IP–адреса, то они не могут прямо, без соответствующей адаптации подключиться к Internet. Существует множество решений, обеспечивающих совместимость. Наиболее популярными являются следующие:

-     преобразование существующих протоколов (IPX, NetBEUI, AppleTalk или других) в IP–протокол с официальным адресом;

-     преобразование внутренних IP–адресов в официальные IP–адреса;

-     установка специальных IP–шлюзов на серверы;

-     использование виртуальной IP–маршрутизации;

-     использование универсальной техники туннелирования.

Первый способ, по крайней мере концептуально, понятен, поэтому остановимся вкратце на остальных.

     Преобразование внутренних  IP-адресов в официальные необходимо в том случае, когда частная сеть базируется на IP-протоколе. Для внутренней адресации обычно используются адреса класса В, которые лежат в диапазоне 192.168.0.0 - 192.168.255.255, что позволяет идентифицировать 65536 узлов. Преобразование адресов для всей корпоративной сети не является необходимым, так как официальные IP-адреса могут сосуществовать с внутренними в коммутаторах и маршрутизаторах сети предприятия. Другими словами, сервер с официальным IP-адресом по-прежнему доступен клиенту частной сети через локальную инфраструктуру. Наиболее часто используют технику разделения небольшого блока официальных адресов многими пользователями. Она подобна разделению пула модемов, поскольку также опирается на предположение, что не все пользователи одновременно нуждаются в доступе к Internet. Здесь существуют два индустриальных стандарта: протокол динамической конфигурации хостов (Dynamic Host Configuration Protocol - DHCP) и трансляция сетевых адресов (Network Adress Translation - NAT), подходы которых слегка различаются. DHCP «сдает» узлу адрес в аренду на время, определяемое администратором сети, тогда как NAT транслирует внутренний IP-адрес в официальный динамически, на время сеанса связи с Internet.

Другим способом сделать частную сеть совместимой с  Internet является установка IP–шлюза. Шлюз транслирует не IP–протоколы в  IP-протоколы и наоборот. Большинство сетевых операционных систем, использующих нативные протоколы, имеют программное обеспечение для IP–шлюза.

Сущность виртуальной IP–маршрутизации заключается в расширении частных маршрутных таблиц и адресного пространства на инфраструктуру (маршрутизаторы и коммутаторы) Internet–провайдера. Виртуальный IP–маршрутизатор является логической частью физического IP–маршрутизатора, принадлежащего и функционирующего у сервис-провайдера. Каждый виртуальный маршрутизатор обслуживает определенную группу пользователей.

Однако, пожалуй, самым лучшим способом обеспечить совместимость можно с помощью методов туннелирования. Эти методы наряду с различной техникой инкапсуляции уже давно используются для передачи по общей магистрали мультипротокольного потока пакетов. В настоящее время эта испытанная технология оптимизирована для Internet–базированных VPN.

Основными компонентами туннеля являются:

-     инициатор туннеля;

-     маршрутизируемая сеть;

-     туннельный коммутатор (опционально);

-     один или более туннельных терминаторов.

Туннелирование должно выполняться на обоих концах сквозного канала. Туннель должен начинаться туннельным инициатором и завершаться туннельным терминатором. Инициализация и завершение туннельных операций может выполняться различными сетевыми устройствами и программным обеспечением. Например, туннель может быть инициирован компьютером удаленного пользователя, на котором установлены модем и необходимое для VPN программное обеспечение, фронтальным маршрутизатором филиала корпорации или концентратором доступа к сети у сервис-провайдера.

Для передачи по Internet пакетов, отличных от IP сетевых протоколов, они со стороны источника инкапсулируются в IP–пакеты. Наиболее часто применяемый метод создания VPN–туннелей заключается в инкапсуляции не IP–пакета в пакет PPP (Point-to-Point Protocol) с последующей инкапсуляцией в IP–пакет. Напомним, что PPP–протокол используется для соединения типа точка-точка, например, для связи клиента с сервером. Процесс IP–инкапсуляции включает добавление стандартного IP–заголовка к оригинальному пакету, который затем рассматривается как полезная информация. Соответствующий процесс на другом конце туннеля удаляет IP–заголовок, оставляя неизменным оригинальный пакет. Протокол PPP обеспечивает сервис на уровне 2 эталонной модели OSI, поэтому такой подход называется туннелирование на уровне 2 (L2 Tunneling Protocol – L2TP). Сегодня довольно широкое распространение получил протокол Point-to-Point Tunneling Protocol, разработанный компаниями 3Com и Microsoft, который поставляется вместе с операционными системами Windows 95 и Windows NT .

Поскольку технология туннелирования достаточно проста, она является и наиболее приемлемой в отношении стоимости.

**4.2. БЕЗОПАСНОСТЬ.**

Обеспечение необходимого уровня безопасности часто является основным пунктом при рассмотрении корпорацией возможности использования Internet–базированных VPN. Многие IT–менеджеры привыкли к изначально присущей частным сетям защите конфиденциальной информации и рассматривают Internet как слишком «общедоступную» для использования ее в качестве частной сети. Однако при условии принятия необходимых мер Internet–базированные виртуальные частные сети могут стать более безопасными, чем VPN, базирующиеся на PSTN. Если пользоваться английской терминологией, то существуют три «Р», реализация которых в совокупности обеспечивает полную защиту информации. Это:

       Protection - защита ресурсов с помощью брандмауэров (firewall);

       Proof - проверка идентичности (целостности) пакета и аутентификация отправителя (подтверждение права на доступ);

       Privacy - защита конфиденциальной информации с помощью шифрования.

Все три «Р» в равной степени значимы для любой корпоративной сети, включая и VPN. В сугубо частных сетях для защиты ресурсов и конфиденциальности информации достаточно использования довольно простых паролей. Но как только частная сеть подключается к общедоступной, ни одно из трех «Р» не может обеспечить необходимую защиту. Поэтому для любой VPN во всех точках ее взаимодействия с сетью общего пользования должны быть установлены брандмауэры, а пакеты должны шифроваться и выполняться их аутентификация.

Брандмауэры являются существенным компонентом в любой VPN. Они пропускают только санкционированный трафик для доверенных пользователей и блокируют весь остальной. Иными словами, пересекаются все попытки доступа неизвестных или недоверенных пользователей. Эта форма защиты должна быть обеспечена для каждого сайта и пользователя, поскольку отсутствие ее в каком-либо месте означает отсутствие везде. Для обеспечения безопасности виртуальных частных сетей применяются специальные протоколы. Эти протоколы позволяют хостам «договориться» об используемой технике шифрования и цифровой подписи, что позволяет сохранить конфиденциальность и целостность данных и выполнить аутентификацию пользователя.

Протокол Microsoft Point-to-Point Encryption (MPPE) шифрует PPP–пакеты на машине клиента перед тем, как направить их в туннель. Версия с 40-битовым ключом поставляется с Windows 95 и Windows NT  (существует также версия со 128-битовым ключом). Сессия шифрования инициализируется во время установления связи с туннельным терминатором по протоколу PPP.

Протоколы Secure IP (IPSec) являются серией предварительных стандартов, разрабатываемых Группой инженерных проблем Internet (Internet Engineering Task Force - IETF). Группа предложила два протокола: Authentication Header (AH) и Encapsulating Security Payload (ESP). Протокол AH добавляет цифровую подпись к заголовку, с помощью которой выполняется аутентификация пользователя, и обеспечивает целостность данных, отслеживая любые изменения в процессе их передачи. Этот протокол защищает только данные, оставляя адресную часть IP–пакета неизменной. Протокол ESP, напротив, может шифровать либо весь пакет (Tunnel Mode), либо только данные (Transport Mode). Эти протоколы используются как раздельно, так и в комбинации.

Для управления безопасностью применяют индустриальный стандарт RADIUS (Remote Authentication Dial-In User Service), представляющий собой базу данных пользовательских профилей, которые содержат пароли (аутентификация) и права доступа (авторизация).

Средства обеспечения безопасности далеко не ограничиваются приведенными примерами. Многие производители маршрутизаторов и брандмауэров предлагают свои решения. Среди них – Ascend, CheckPoint и Cisco.

**4.3. ДОСТУПНОСТЬ.**

Доступность включает три в равной степени важные составляющие:  время предоставления услуг, пропускную способность и время задержки. Время предоставления услуг является предметом договора с сервис-провайдером, а остальные две составляющие относятся к элементам качества услуг (Quality of Service - QoS). Современные технологии транспорта позволяют построить VPN, удовлетворяющие требованиям практически всех существующих приложений.

**4.4. УПРАВЛЯЕМОСТЬ.**

Администраторы сетей всегда хотят иметь возможность осуществлять сквозное, из конца в конец, управление корпоративной сетью, включая и ту часть, которая относится к телекоммуникационной компании. Оказывается, что VPN предоставляют в этом плане больше возможностей, чем обычные частные сети. Типичные частные сети администрируются «от границы до границы», т.е. сервис-провайдер управляет сетью до фронтальных маршрутизаторов корпоративной сети, в то время как абонент управляет собственно корпоративной сетью до устройств доступа к WAN. Технология VPN позволяет избежать этого своеобразного разделения «сфер влияний», предоставляя и провайдеру, и абоненту единую систему управления сетью в целом, как ее корпоративной частью, так и сетевой инфраструктурой общедоступной сети. Администратор сети предприятия имеет возможность выполнять мониторинг и реконфигурацию сети, управлять фронтальными устройствами доступа, определять состояние сети в режиме реального времени.

**4.5. АРХИТЕКТУРА VPN.**

Существуют три модели архитектуры виртуальных частных сетей: зависимая, независимая и гибридная как комбинация первых двух альтернатив. Принадлежность к той или иной модели определяется тем, где реализуются четыре основных требования, предъявляемых к VPN. Если провайдер сетевых глобальных услуг предоставляет полное решение  для VPN, т.е. обеспечивает туннелирование, безопасность, производительность и управление, то это делает архитектуру зависимой от него. В этом случае все процессы в VPN для пользователя прозрачны, и он видит только свой нативный трафик – IP-, IPX- или NetBEUI–пакеты. Преимущество зависимой архитектуры для абонента заключается в том, что он может использовать существующую сетевую инфраструктуру «как она есть», добавляя лишь брандмауэр между VPN и частной WAN/LAN.

Независимая архитектура реализуется в том случае, когда организация обеспечивает все технологические требования на своем оборудовании, делегируя сервис-провайдеру лишь транспортные функции. Такая архитектура обходится дороже, однако предоставляет пользователю возможность полного контроля за всеми операциями.

Гибридная архитектура включает зависимые и независимые от организации (соответственно, от сервис-провайдера) сайты.

Какие же коврижки сулят VPN для корпоративных пользователей? Прежде всего, по оценкам индустриальных аналитиков, это снижение расходов на все виды телекоммуникаций от 30 до 80 %. А также это практически повсеместный доступ к сетям корпорации или других организаций; это реализация безопасных коммуникаций с поставщиками и заказчиками; это улучшенный и расширенный сервис, недостижимый в сетях PSTN, и многое другое. Специалисты рассматривают виртуальные частные сети как новую генерацию сетевых коммуникаций, а многие аналитики считают, что VPN вскоре заменят большинство частных сетей, базирующихся на арендуемых линиях.

ЗАКЛЮЧЕНИЕ.

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN">

***Internet: эволюция философии защиты.***

Проблема защиты информации в Internet ставится и, с той или иной степенью эффективности, решается с момента появления сетей на основе протоколов семейства TCP/IP.

В эволюциях технологий защиты можно выделить три основных направления. Первое — разработка стандартов, имплиментирующих в сеть определенные средства защиты, прежде всего административной. Примером являются IP security option и варианты протоколов семейства TCP/IP, используемые в Министерстве обороны США. Второе направление — это культура межсетевых экранов (firewalls), давно применяемых для регулирования доступа к подсетям. Третье, наиболее молодое и активно развивающееся, направление — это так называемые технологии виртуальных защищенных сетей (VPN, virtual private network, или intranet).

Наблюдаемый в последние годы взрывной рост популярности Internet и связанных с ней коммерческих проектов послужил толчком для развития нового поколения технологий защиты информации в TCP/IP-сетях. Причем если ранее, вплоть до начала 90-х, основной задачей защиты в Internet было сохранение ресурсов преимущественно от хакерских атак, то в настоящее время актуальной становится задача защиты коммерческой информации.

Качественно это совершенно разные виды защиты. Атакующая коммерческую информацию сторона может позволить себе большие затраты на взлом защиты и, следовательно, существенно более высокий уровень: наблюдение трафика, перехват информации, ее криптоанализ, а также разного рода имитоатаки, диверсии и мошенничества.

Наивные способы защиты, такие как запрос пароля с последующей передачей его в открытом виде по коммуникационному каналу и списки доступа на серверах и маршрутизаторах, становятся в этих условиях малоэффективными. Что же может быть противопоставлено квалифицированной и технически вооруженной атакующей стороне? Конечно же, только полноценная, криптографически обеспеченная система защиты.

Предложений подобных средств на рынке Internet достаточно много. Однако по ряду параметров ни одно из них не может быть признано адекватным задачам защиты информации именно для Internet. Например, достаточно криптостойкой и замечательной по своей идее формирования «паутины доверия» является распространенная система PGP (Pritty good privacy). Однако, поскольку PGP обеспечивает шифрование файлов, она применима только там, где можно обойтись файловым обменом. Защитить, допустим, приложения on-line при помощи PGP затруднительно. Кроме того, уровень защиты PGP слишком высок. Стыковка защиты PGP с другими прикладными системами потребует определенных усилий, если, конечно, вообще окажется осуществимой.

Выбор технологии защиты информации для большой открытой системы — сети масштаба Internet, крупной корпоративной сети, сети коммуникационного провайдера, должен удовлетворять ряду специфических требований:

·     наличие *открытой* спецификации, отсутствие монополизма в части технологических решений

·     *широкая масштабируемость* решений по техническим и ценовым параметрам

·     *универсальность технологии, переносимость, многоплатформенность*

·     *совместимость* аппаратных, программных, коммуникационных решений

·     обеспечение, при необходимости, *комплексной* защиты информации

·     простота управления ключами и организации защищенных коммуникаций для вновь подключенных пользователей.

Полноценное использование сервера требует его подключения через местный маршрутизатор, который станет одним из рубежей защиты. Маршрутизатор можно запрограммировать таким образом, что он будет блокировать опасные функции и разрешать передачу поступающих извне запросов только в специально назначенные серверы.

Частичную защиту обеспечивает блокировка портов, реализуемая в большинстве современных маршрутизаторов путем формирования списков контроля доступа на основе языка команд маршрутизатора. Еще один способ защиты - сконфигурировать маршрутизатор так, чтобы он разрешал соединения из Internet только с теми компьютерами сети, информация на которых открыта для всеобщего пользования. Остальные части сети изолируются от этих компьютеров брандмауэрами или иными средствами. Такой способ защиты используется многими крупными корпорациями.

По своим функциям к маршрутизаторам примыкают автономные пакеты фильтрации трафика, устанавливаемые на ПК или рабочих станциях. Типичным продуктом этого класса является ПО FireWall-1 компании CheckPoint Software Technologies, инсталлируемое на рабочие станции фирмы Sun и выполняющее фильтрацию входного и выходного потоков. FireWall-1 в отличие от маршрутизаторов способен динамически открывать пути передачи данных в соответствии с протоколами Internet, например с FTP. Кроме того, данный пакет снабжен удобным в работе графическим интерфейсом, средствами оповещения об угрозе взлома системы защиты и средствами регистрации доступа к сети, генерирующими сообщения о необычных действиях. Подобные продукты, как правило, обеспечивают лучшую защиту по сравнению с маршрутизаторами, но отличаются высокой стоимостью. Брандмауэры Маршрутизаторы и продукты типа только что рассмотренного ПО FireWall-1 не имеют некоторых функций, повышающих степень защищенности от опасных вторжений в сеть. Например, при передаче потока данных они не анализируют его содержимое и не в состоянии осуществлять проверку полномочий на доступ к ресурсам сети. Такими возможностями обладают брандмауэры - выделенные компьютеры с активными функциями фильтрации информационных потоков в точке связи локальной сети с внешним миром. Основная задача систем этой категории - изолировать сеть от посягательств извне путем просмотра пакетов данных, блокировки "подозрительных" видов трафика и использования специальных средств подтверждения полномочий на доступ. Таким образом, брандмауэр выступает в роли сторожа, не пропускающего любые входные или выходные данные, которые не соответствуют явно сформулированным критериям. Сегодня на рынке имеется широкий выбор средств защиты данных на основе брандмауэров.