Вступление

На сегодняшний день мелкие и средние фирмы при проектировании своих сетей часто не задумываются о необходимости их защиты. Такие сети, как правило, насчитывают до двухсот компьютеров и не имеют реальной необходимости в защите от атак профессионалов, поэтому в таких сетях требования к защите не являются очень высокими. При этом основными угрозами для них являются:

* Неумышленные действия и ошибки собственных сотрудников (по незнанию, из любопытства, случайно и т.п.);
* Различные неполадки и сбои;
* Стихийные бедствия;
* Непрофессиональная атака со стороны конкурентов.

Основной проблемой при защите сетей небольших предприятий является необходимость изучения большого объема литературы из-за разбросанности по разным книгам различных аспектов такой защиты. Кроме того, подход большинства книг неконкретен и описывает проблему только в общем, в то время как обсуждаемые фирмы имеют сети вполне определенной конфигурации с вполне определенным программным обеспечением. Таким образом, эти фирмы нуждаются в конкретных инструкциях, затрагивающих все аспекты безопасности небольших сетей, не разбросанных по разным источникам и не затрагивающих особо широкий спектр вопросов.

* большое количество документации и хорошая техническая поддержка.

Такая типовая сеть состоит из следующих компонентов: до 200 рабочих станций, соединенных с использованием топологии “звезда”; один или несколько концентраторов или коммутаторов; главный и резервный контроллеры домена Windows NT. Для соединений используется витая пара 5 категории, т.е. сеть строится по технологии 10BaseT или 100BaseT.

Организации среднего масштаба обычно имеют выделенный канал связи с сетью Интернет, для обеспечения работы с которым устанавливается прокси-сервер. Также, в случае наличия выделенного канала организация обычно имеет Web-сервер и почтовый сервер.

При небольшом количестве компьютеров нет смысла использовать модель сети с несколькими доменами Windows NT, поэтому все компьютеры входят в один домен.

В этой типовой сети можно выделить несколько направлений, по которым злоумышленник может получить несанкционированный доступ к информации либо нарушить нормальное функционирование ЛВС. Кроме злоумышленных действий, при построении сети необходимо также обезопасить ее от таких явлений, как отключения и перепады напряжения, пожары, наводнения, сбои и отказы в оборудовании и т.п.

Таким образом, в данной сети можно выделить следующие направления, имеющие значение с точки зрения защиты информации:

1. Защита на физическом уровне от сбоев и отказов отдельных компьютеров и их компонентов.
2. Защита от доступа к компьютерам пользователей, не имеющих на это права.
3. Защита от несанкционированного использования компьютеров, в т.ч. кражи и установки комплектующих и других устройств, а также несанкционированного копирования и съема информации с компьютера.
4. Защита от съема информации с кабельных соединений и защита от несанкционированного физического подключения к ЛВС.
5. Настройка и установка программного обеспечения в соответствии с политикой безопасности предприятия, а также для максимально возможного предотвращения ущерба в случае неожиданного поведения программ. Здесь должны учитываться как непреднамеренные (ошибки и сбои в программах), так и преднамеренные (вирусы, «троянские кони», «логические бомбы» и т.п.) случаи неожиданного поведения.
6. Защита с помощью политики групп. Это означает, что группы и учетные записи пользователей домена создаются и ведутся в строгом соответствии с политикой безопасности предприятия. Также в соответствии с данной политикой им даются соответствующие права, т.е. используется разграничение доступа на уровне пользователей.
7. Правильная настройка Web- и Mail-серверов для минимизации возможностей злоумышленнику нарушить нормальную работу сети или получить несанкционированный доступ к информации, используя «дыры» в ПО этих серверов.
8. Правильная настройка прокси-сервера для контроля входящих и исходящих соединений, а в итоге - для минимизации возможностей злоумышленнику получить несанкционированный доступ к локальной сети предприятия или нарушить ее нормальную работу из сети Интернет.

В последующих главах будут подробно рассмотрены все перечисленные выше пункты.

Следует еще раз заметить, что в качестве операционных систем серверов и рабочих станций нашей типовой сети, а также в качестве ПО серверов используются программные продукты фирмы Microsoft, так как их использование позволяет удовлетворить большинству потребностей предприятий среднего и малого бизнеса.

Для упрощения дальнейшего чтения материала ниже приведен список используемого в сети программного обеспечения.

1. В качестве ОС рабочих станций сети - MS Windows 95, MS Windows 98, MS Windows NT 4.0 Workstation + Service Pack 6 или MS Windows 2000 Professional.
2. В качестве ОС серверов сети - MS Windows NT 4.0 Server + Service Pack 6.
3. В качестве ПО Web-сервера - MS Internet Information Server 3.0.
4. В качестве ПО почтового сервера - MS Exchange 5.5.
5. В качестве ПО прокси-сервера - MS Proxy Server 2.0.

Разумеется, кроме этих программных продуктов, пользователи могут работать и с другими, но в дальнейшем изложении подразумевается, что перечисленные выше программные продукты используются обязательно.

# Обеспечение защищенности информации при сбоях и отказах отдельных компьютеров и их компонентов

Потери информации в результате отказов компьютеров и их компонентов происходят довольно часто. Однако почему многие организации не обращают на это должного внимания, не предпринимая никаких усилий для предотвращения потерь в результате, например, скачков и отключений электроэнергии, пожаров и т.д.

Ниже мы рассмотрим, что следует считать обязательным для рассматриваемой нами типовой организации с точки зрения данной проблемы.

## Надежность сервера

Надежность является одним из самых важных критериев выбора сервера. В серверах, по сравнению с обычными ПК, надежности аппаратных компонентов уделяется значительно большее внимание. Они проходят более тщательный отбор и тестирование, ведь выход из строя сервера приведет к прекращению работы десятков пользователей. Сейчас для серверов нередко используют технологии, которые ранее были привилегией корпоративных машин.

По данным статистики, наиболее часто выходят из строя механические детали, в первую очередь дисководы и вентиляторы. Блоки питания, микросхемы оперативной памяти, контроллеров и сетевых плат ломаются реже. Поломки центральных процессоров (если это не связано с проблемами охлаждения) случаются редко.

Следовательно, меры по повышению надежности должны быть сконцентрированы на самых уязвимых компонентах.

Для исключения проблем с охлаждением в серверах устанавливают избыточные вентиляторы. Но это характерно для машин старшего и отчасти среднего уровня. Более того, при выходе из строя вентилятора серверы солидных производителей способны генерировать сигналы тревоги. Некоторые модели серверов при превышении порогового значения температуры автоматически отключаются, чтобы не было более тяжких последствий.

Самым популярным способом повышения надежности дисковой подсистемы является применение массивов RAID с горячей заменой дисков, особенно по спецификации RAID-5 и RAID-3. Более изощренные и надежные спецификации, такие, как RAID-53, не нашли применения в системах начального и среднего уровня.

К сожалению, применение массивов RAID далеко не всегда гарантирует надежность дисковой подсистемы. Особенно это касается самых современных дисковых накопителей SCSI с частотой вращения 10 000 об/мин. Дело в том, что подобные диски очень сильно нагреваются в процессе работы (до 70 градусов Цельсия). За эту особенность их иногда называют утюгами. Если дисководы размещены в посадочных слотах близко друг от друга, то из-за плохой вентиляции они часто выходят из строя. Поэтому последние версии SCSI-дисков лучше устанавливать с зазором между ними. Некоторые, хотя далеко не все дисководы снабжаются собственными вентиляторами.

Все системы старшего уровня и многие среднего уровня допускают установку дублированных блоков питания (обычно данная опция предоставляется факультативно). Однако большинство администраторов не видит в этом необходимости. И, наверное, зря. Если к каждому блоку питания подключить собственный источник бесперебойного питания, то это значительно уменьшит для серверов возможность потери электропитания при выходе из строя как блока питания, так и ИБП.

Во многих серверах (даже начального уровня) устанавливают микросхемы оперативной памяти с коррекцией ошибок (ECC). Но реально фирменные микросхемы солидных производителей редко выходят из строя в процессе работы сервера (что привело бы к запуску механизма коррекции ошибок). Обычно микросхемы выходят из строя при перевозке или при установке в сервер, т. е. до начала его работы. К тому же память ECC слишком дорога. В большинстве своем для серверов годятся обычные микросхемы памяти с контролем четности. Но для критических применений (там, где недопустимы перерывы в работе сервера) лучше перестраховаться и использовать память ECC.

### Рекомендации по выбору серверов

Как правило, выбор серверов для организации – непростая задача. Выбор зависит от функций сервера, от требуемого уровня его надежности, от финансовых возможностей организации и т.п. Тем не менее, существует несколько общих моментов с точки зрения защищенности информации, хранимой на сервере и его надежного функционирования.

1. Следует рассмотреть возможность покупки «фирменных» серверов таких производителей, как Compaq, Dell, IBM и т.п. Если клиентские машины могут быть дешевыми, неизвестно какой сборки, то к выбору сервера следует подойти более ответственно. Даже если сервер будет стоить в несколько десятков раз дороже типичной клиентской машины, это окупится его более высокой надежностью и производительностью. В том случае, если покупка дорогой машины невозможна, следует выбирать компоненты с повышенной надежностью, в первую очередь – жесткие диски, материнские платы, устройства бесперебойного питания.
2. Для файловых серверов и серверов баз данных просто необходимы устройства резервного копирования. Здесь трудно дать какие-либо конкретные рекомендации, так выбор средств резервного копирования зависит от объемов хранимых данных. Обычно резервное копирование осуществляют на магнитные ленты или МО-диски.
3. Для серверов желательны схемы с избыточностью компонентов. Рекомендуется применять схемы с зеркалированием или дублированием дисков, тем более что Windows NT позволяет реализовать некоторые уровни RAID программно. Для повышенных требований к скорости дублирования можно рассмотреть возможность применения аппаратных контролеров RAID. Кроме того, если в качестве сервера организация использует не обычный компьютер, то рекомендуются схемы с несколькими вентиляторами и двумя блоками питания.
4. Следует по возможности применять диски SCSI.
5. Источник бесперебойного питания для сервера просто необходим. Рекомендации по его выбору приведены ниже.
6. В случае, если предъявляются специальные требования, рассмотрите сервера с возможностью «горячей» замены компонентов, памятью ECC и т.п. К сожалению, Windows NT 4.0 очень слабо поддерживает возможность “горячей” замены.

### Рекомендации по выбору клиентских машин

Для клиентских машин необходимо использовать сетевые фильтры типа Pilot, особенно там, где есть лазерные принтеры. Источники бесперебойного питания – еще более лучший выбор.

Частой ошибкой является покупка дешевой материнской платы. Рекомендуется брать платы среднего или высокого ценового диапазона.

## Источники бесперебойного питания

Если условия подачи электричества нестабильны - например, если оборудование подвергается постоянным отключениям (12 и более раз в год) или ему больше 10 лет - сеть оказывается сильно уязвимой со стороны электропитания. В такой ситуации следует подумать о повышении степени защиты (количество и тип защищаемых компонентов сети), а также о типе развертываемых ИБП. Более высокий уровень защиты необходим также в случае, когда повседневная жизнь организации зависит в значительной степени от работы сети.

Потребность защиты станций-клиентов и других сетевых устройств зависит от характера конкретной сетевой среды. В общем случае источник питания клиентской рабочей станции обеспечивает адекватную защиту электропитания. Однако, если в клиентской среде выполняются важные приложения типа расчета платежной ведомости, мониторинга ухода за больными и учета продаж, им может потребоваться защита средствами ИБП, особенно если программное обеспечение клиента локально запоминает в оперативной памяти данные, используемые для последующей обработки. При решении вопроса о защите концентраторов и коммутаторов выясните, насколько критичен каждый компонент для общего функционирования сетевой структуры. Если уж вам нужно защищать клиентов, то следует также защитить и сетевую магистраль для сохранения взаимодействия между клиентами и сервером. Даже если вы решите не защищать клиентов, все равно стоит обдумать возможность установки ИБП для обеспечения электропитания магистрали, тем более, если серверам необходимо сопряжение посредством сети. Но предположим, вы сочли, что острой нужды в защите станций-клиентов и устройств на магистрали сети средствами ИБП все-таки нет, - тогда, по крайней мере, обеспечьте их защиту с помощью предохранителей и регуляторов напряжений.

Как только вы определили, какие компоненты следует защищать, нужно также принять решение о типах развертываемых ИБП. Для выбора имеются три типа устройств: автономные, интерактивные или линейно-интерактивные. Все типы ИБП обеспечивают базовые функции защиты, однако более изощренные интерактивные и линейно-интерактивные системы предоставляют средства для компенсации отклонений напряжения. Повторимся, тип выбираемого ИБП зависит от капризов электропитания конкретной среды и чувствительности компонентов сети и циркулирующей в ней информации.

Автономные ИБП обеспечивают минимальную защиту сетевых устройств только на случай отключения питания. Исчезновение напряжения приводит к активизации батарей автономного ИБП, тем самым обеспечивая работу оборудования до исчерпания заряда аккумуляторов. Являясь, по сути дела, только резервным источником питания, эти устройства дешевле двух других типов ИБП. Если электропитание оборудования хорошего качества, то автономные ИБП способны предоставить необходимый уровень защиты.

Автономный ИБП защищает аппаратные компоненты только от исчезновения напряжения, при этом питание осуществляется от батарей ИБП. Продолжительность времени, в течение которого ИБП может обеспечивать работу защищаемого оборудования, зависит от емкости батареи. Интерактивные ИБП - наиболее дорогие устройства бесперебойного питания - защищают критически важное оборудование посредством непрерывной регенерации синусоидальной волны источника питания. Эта операция аналогична функции, выполняемой повторителем, получающим и регенерирующим цифровые сигналы перед дальнейшей их отправкой по каналу связи. По существу, эти устройства "очищают" напряжение, подаваемое компонентам сети. Интерактивные ИБП обеспечивают питание защищаемых ими устройств при любых условиях и непрерывно перезаряжают свои батареи; они всегда готовы среагировать на проблемы, связанные с подачей питания. Интерактивные ИБП также улучшают качество источника питания за счет регулировки напряжения, что необходимо в случае, если планируется использовать резервные генераторы.

Интерактивные ИБП, наилучшим образом приспособленные для поддержки особо важных компонентов сети, подают энергию защищаемым устройствам при всех условиях и "очищают" электрический ток путем постоянной регенерации синусоидальной волны источника питания.

Линейно-интерактивный ИБП представляет собою гибрид интерактивных и автономных ИБП. При нормальной работе инвертор фильтрует ток в цепи, подаваемый на вход защищаемого устройства, и поддерживает батареи в полностью заряженном состоянии. Если напряжение пропадает, инвертор выполняет обратную операцию, преобразовывая постоянный ток батареи в переменный. Линейно-интерактивные модели ИБП лучше всего приспособлены для поддержки не особенно важных элементов сети, например файловых и принт-серверов.

Линейно-интерактивные ИБП сохраняют свои батареи в заряженном состоянии посредством фильтрации тока в цепи защищаемых устройств. Когда напряжение пропадает, инвертор ИБП преобразует постоянный ток в переменный, обеспечивая подачу резервного напряжения к защищаемым компонентам.

Если ИБП больше десятка, то эффективный способ их контроля и управления насущно необходим. К счастью, большинство производителей ИБП предоставляет вместе со своими системами управляющее ПО. Управляемые источники бесперебойного питания обычно называются интеллектуальными (smart). Подобные устройства могут регистрировать события, непрерывно контролировать качество энергоснабжения, сообщать о состоянии батарей и выполнять другую диагностику. Они также автоматически выгружают с сервера операционную систему в случае, когда продолжительность отсутствия напряжения превышает время автономной работы ИБП. С помощью управляющего ПО при отключении питания работу сети можно автоматически свертывать. При продолжительных перерывах в питании программное обеспечение должно автоматически оповещать пользователей и технический персонал, сохранять открытые файлы и закрывать приложения до остановки пострадавшего сервера.

В зависимости от производителя программное обеспечение управления питанием выдает предупреждения в виде звуковых сигналов, электронной почты и пейджинга. Некоторые пакеты позволяют перепрограммировать сообщения, посылаемые пользователям и/или техническому персоналу. Чтобы эти системы работали правильно, программное обеспечение управления питанием должно быть полностью совместимым с вашей сетевой ОС. Большинство производителей поддерживают системы NetWare и Windows NT.

Ниже рассмотрен список критериев, которые следует учитывать при определении требований и выборе конкретного ИБП.

Величина нагрузки. Наиболее простым критерием выбора ИБП является величина нагрузки (мощность), измеряемая в киловольт-амперах (kVA). Этот показатель представляет собой количество энергии, необходимое защищаемому устройству для нормальной работы. Мощность устройства можно грубо оценить, используя следующую формулу: кВА = вольты·амперы/1000. Вольты обозначают величину напряжения, требуемого для работы устройства (например, 110 вольт); амперы обозначают величину постоянного тока, указанную в паспорте устройства. Чем выше значение кВА, тем более мощный и дорогой ИБП вам необходим. Надежный ИБП - тот, у которого значение мощности (кВА) выше вычисленного значения на 20-50%.

Время работы батареи. Этот показатель обозначает период времени, в течение которого ИБП обеспечивает электропитание (при определенной величине нагрузки) защищаемого устройства. В общем случае время работы батареи следует принять равным, по крайней мере, 15 минутам. Иначе гарантировать работу компонентов сети в течение периода, превышающего обычную продолжительность отключения питания, весьма проблематично. Если этого недостаточно, выберите ИБП с возможностью наращивания емкости батарей - и рассмотрите возможность приобретения резервного генератора. Требования к качеству питания. В случае отключения энергоснабжения все ИБП обеспечивают питание от батарей в течение непродолжительного периода времени. Однако убедитесь в том, что ИБП надлежащим образом улучшают характеристики напряжения переменного тока в случае подачи питания от электросети. Если шум линий имеет место, выбранный ИБП должен содержать блок подавления шума; если напряжение подвержено спадам, ИБП должен обеспечивать регулировку напряжения. В любом случае встроенная защита от скачков напряжения для ИБП обязательна. Даже если выбросы напряжения, происходящие по вине обслуживающей коммунальной компании, в вашей практике редкость, позаботиться о защите от скачков напряжения все-таки стоит, поскольку при возникновении скачков оборудование может сгореть.

Рекомендации по выбору и установке источников бесперебойного питания

Рекомендуется составить план сети и с его помощью определить, какие из компонентов нуждаются в источниках бесперебойного питания. Для нашей типовой схемы следует установить их на сервера, на коммутаторы (концентраторы), на устройство сопряжения с сетью Интернет. Если необходимо, следует установить ИБП на клиентские машины, где обрабатываются важные данные, на компьютеры руководителей.

Рекомендуется выбирать однотипные ИБП. Желательным условием является наличие ПО, способного удаленно управлять и контролировать разбросанные по зданию источники питания. Необходимо настроить ПО ИБП на посылку предупреждений администратору при отключении питания электросети и разряде батарей, а также на автоматическое корректное завершение работы ОС при разряде батарей.

# Организационная защита

Организационная защита является очень эффективным методом обеспечения сохранности информации. Под ней понимается довольно широкая область, однако для рассматриваемых нами типовых организаций можно выделить несколько ключевых моментов.

## Ограничение доступа в здание и помещение

Рекомендуется пост охраны на входе, использование пропускной системы.

Помещения должны запираться и иметь сигнализацию. Сигнализация должна быть установлена на двери и окнах, возможно применение датчиков движения.

## Ограничение свободного доступа к серверам и коммутационному оборудованию

Это обеспечивается использованием таких мер, как ограничение доступа в помещения, где находятся компьютеры с наиболее ценной информации. Как правило непосредственная защита путем ограничения доступа организуется для сервера. Если невозможно размещение сервера в отдельном помещении, то используются шкафы или запираемые корпуса.

Доступ к серверам должен быть возможен только администратору, руководителю, оператору резервного копирования.

## Защита от кражи и подмены оборудования

В тех случаях, где эта проблема актуальна, лучше использовать для компьютеров специальные корпуса. Если это невозможно, корпус компьютера должен быть опечатан. Рекомендуется также проверять целостность оборудования при сдаче рабочего места.

Обычно такая проблема возникает при необходимости предоставлять доступ к компьютерам внештатных сотрудников, гостей, командированных и т.д. Здесь крайне важно отсутствие так называемой «обезлички», т.е. должно быть известно кто последний работал на данном компьютере. Обычно это достигается применением специальных программ либо записью в журнале.

Периодически необходимо проверять соответствие комплектующих, серийные номера. Кстати, в компьютер могут быть установлены специальные устройства, записывающие и передающие информацию. Так как такое оборудование довольно дорого, это может означать, что за вашей организацией ведется направленный шпионаж.

## Защита от несанкционированного съема информации с экрана дисплея.

Это пункт обеспечивается также использованием организационных мер. Необходимо правильное планирование размещения компьютерной техники. Мониторы, по возможности, разворачиваются от окон, дверей.

Также используются программные средства. Основная проблема безопасности заключается в том, что человек отходя от своего рабочего места оставляет компьютер не заблокированным. Для снижения вероятности получения информации таким методом необходимо использование заставок "save-screen" с паролем. Т.е. после включения заставки получить доступ к компьютеру можно только введя пароль. Данная операция не требует от пользователя сложных действий.

## Резервное копирование

Данная операция также должна быть отнесена к организационной защите.

Для ее проведения необходим план резервного копирования. Наиболее распространенным является полное резервное копирование раз в неделю и инкрементирующее каждый день. Носители, на которые производится полное резервное копирование, следует чередовать в течение некоторого времени, обычно месяца. Для применения инкрементирующего копирования в течение недели применяют разные носители на каждый день недели.

Хранить носители резервного копирования следует в несгораемых сейфах. Рекомендуется хранить их в другом здании.

Перед началом применения регулярного резервного копирования следует попытаться восстановить резервные данные и убедиться, что в случае потери информации ее это можно будет сделать без труда.

Для рассматриваемой нами типовой сети следует производить копирование основного контроллера домена (PDC) Windows NT, информация почтового сервера, возможно – Web-сервера. Рекомендуется сохранять важную информацию с серверов баз данных и файловых серверов.

Обычно в такой небольшой сети операцию резервного копирования производит администратор. Однако при большом объеме работы или его сильной загруженности этим может заниматься и оператор резервного копирования. В любом случае ситуация с резервным копированием должна быть под контролем сетевого администратора.

## Парольная защита

Как известно, наиболее популярная система разграничения доступа – паролирование. Система Windows NT позволяет довольно гибко настраивать ограничения на выбор пароля, однако организационные меры здесь еще более важны.

Самой большой проблемой здесь является выбор простых и легко угадываемых паролей. Как защититься от этого программными средствами, рассказано ниже, организационные же меры здесь рекомендуются следующие:

1. Следует провести с каждым пользователем небольшой ликбез, объяснив для чего нужен пароль, какие пароли являются надежными, как выбирать надежный легко запоминаемый пароль, зачем их периодически нужно менять.
2. Следует постоянно проверять наличие у рабочих мест свободно лежащих бумажек с паролями. Для злостных нарушителей следует предусмотреть меры воздействия и наказания.
3. Администратор должен периодически проверять наличие быстро вскрываемых паролей и предупреждать об этом пользователей.

## Другие организационные моменты

При приеме на работу каждый служащий должен подписать соглашение о неразглашении коммерческой тайны, которое может быть включен в контракт или трудовой договор.

Часто администратор ЛВС сталкивается с непониманием со стороны пользователей, которые не выполняют требования по защите информации. Здесь необходимо проявлять жесткость. Руководитель предприятия должен поддерживать в этом сетевого администратора.

При требовании выполнения организационных мер хорошим приемом является ссылка на вышестоящие организации или руководство, которые «обещают уволить и администратора, и служащего при малейшем нарушении».

# Защита кабельных соединений

## 

## Кабель типа «витая пара»

Кабель типа «неэкранированная витая пара» для сетей состоит из четырех пар проводов 24-го сортамента. По проводам пары передаются сигналы противоположной полярности, поэтому для каждой пары суммарная передаваемая мощность равна нулю. Это позволяет снизить потери за счет электромагнитного излучения и свести к минимуму наводки (перекрестные помехи) от соседних проводов. На принимающем конце сигнал, идущий по «отрицательному» проводу, инвертируется и суммируется с сигналом, идущим по «положительному» проводу. При этом сигнал получается максимальным.

Кабели типа «витая пара» подразделяются на несколько категорий в зависимости от их пропускной способности. Пропускная способность витой пары зависит от точности соблюдения производственной технологии и строгости контроля степени скручивания проводов в процессе производства. Витая пара излучает радиосигналы, длина волны которых кратна длине одного витка. Пара, имеющая виток длиной 10 см, будет излучать первичные интерференционные волны с периодом 10 см.

Если различные пары в составе одного кабеля свиты одинаково, то их излучения будут интерферировать. Поэтому желательно, чтобы разные пары в кабеле имели витки такой длины, которая не приводила бы к образованию гармоник. В этом случае можно снизить помехи, наводимые парами друг в друге. Витые пары подразделяются на следующие категории:

Категория 1. Провода для передачи звуковой информации.

Категория 2. Новый тип проводов для передачи звука и последовательных данных.

Категория 3. Скорость передачи данных достигает 10 Мбайт/с (этого достаточно для сетей типа Ethernet или Token Ring с пропускной способностью 4 Мбайт).

Категория 4. Скорость передачи данных достигает 20 Мбайт/с (этого достаточно для сетей Token Ring с пропускной способностью 16 Мбайт).

Категория 5. Скорость передачи данных достигает 100 Мбайт/с (этого достаточно для сетей типа Fast Ethernet или CDDI).

Категория 6 (перспективная). Скорость передачи данных достигает 155 Мбайт/с (этого достаточно для сетей типа ATM-155).

Неэкранированные витые пары категорий 3 – 5 конструктивно спроектированы так, что не создают помехи друг в друге, но подвержены помехам от внешних источников. Кроме того, данные с них легко считываются с помощью других устройств. Сигналы в проводах витой пары принимаются расположенными вблизи от проводов индукционными усилителями или путем считывания наведенного сигнала (перекрестной помехи) с неиспользуемых пар. Декодирование данных, считанных с проводов, с помощью сетевых анализаторов представляет собой несложную задачу.

Экранированная витая пара довольно надежно защищена от помех, создаваемых внешними источниками, подобно витой паре категории 4. Однако для них актуальной является проблема перекрестных помех, поскольку степень скручивания в них проводов слабо контролируется в процессе производства. Из-за более высокой стоимости экранированная витая пара не очень широко используется в США, но пользуется большим спросом во многих европейских странах.

## Политика применения кабелей типа «витая пара»

Рекомендуется все кабели типа «витая пара», находящиеся вне распределительных шкафов и не помещенные под фальшполами или подвесными потолками, протягивать внутри резиновых или пластиковых труб или пластиковых сетевых магистралей (кабельгонов). Стыки труб и магистралей целесообразно изолировать контровочной лентой или краской, нарушение которых должно указывать на попытки получения доступа к кабелям.

Закрашивайте швы между панелями подвесных потолков так, чтобы любое их несанкционированное вскрытие было заметно. После планового вскрытия нужно сразу же снова закрашивать их.

Рассмотрите возможность прокладки всех сетевых кабелей в потолочных кабельгонах, которые могут быть закрыты или опечатаны.

Все распределительные щиты и коробки должны быть заперты так же, как и помещения, в которых установлены компьютеры.

## Сетевая топология типа «звезда»

Данные сети – самые распространенные на сегодняшний день. В сетях с топологией «звезда» каждый кабель подключается непосредственно к компьютеру и к концентратору. С этой точки зрения звезда представляет собой совокупность двухточечных соединений. По каждому из кабелей идет обмен только с одним компьютером (хотя иногда для разветвления сети в разрывы кабеля могут подключаться концентраторы).

Основные проблемы звездообразных сетей связаны с незащищенностью портов концентратора и возможностью скрытого подключения концентратора вместо компьютера. В обоих случаях к сети без ведома администратора может быть подключен полнофункциональный компьютер. Эту проблему можно частично решить, обезопасив распределительные устройства. Однако выявить несанкционированное подключение концентраторов можно либо с помощью программного обеспечения мониторинга, либо путем прекращения работы всех сетевых компьютеров и последующего мониторинга потерь в каналах связи. На рисунке 2 показан вариант скрытого подключения концентратора в том месте, где должен быть компьютер.

Авторизованный пользователь

Авторизованный пользователь

Авторизованный пользователь

Авторизованный пользователь

Авторизованный пользователь

Авторизованный пользователь

Авторизованный пользователь

Концентратор

Концентратор

Злоумышленник

Сервер

Рисунок 2

## 

## Политика применения сетей типа «звезда»

Надежно перекройте доступ к распределительным шкафам и устройствам.

Поскольку посторонний может просто подключиться к одному из неиспользуемых Ethernet-портов концентратора, необходимо защищать эти порты либо аппаратным путем, либо путем установки сигнальных систем, контролирующих изменение состояния порта SNMP.

Защита неиспользуемых портов необязательно должна быть реализована на самом концентраторе. При изменении конфигурации сети без присмотра обычно остаются сетевые коннекторы. Необходимо внимательно следить, чтобы к таким коммутационным устройствам в незапертых помещениях не подключился никто из посторонних.

Следует всегда отключать неиспользуемые порты коммутатора для физических устройств. При переносе компьютера следует убедиться, что соответствующая сетевая магистраль отключена от концентратора.

# Безопасность сетей на основе Windows NT

## 

## Общие сведения о сетях на основе Windows NT

Для функционирования системы защиты информации от несанкционированного доступа требуется механизм идентификации каждого пользователя. Поэтому в операционной системе Windows NT и построенных на ее основе доменах обязателен процесс входа в систему (logon).

Пользователь, как правило, вводит информацию о себе только раз — при входе в систему, получая после этого доступ к ресурсам, расположенным как в том домене, где он зарегистрирован, так и в других доменах Windows NT. При этом может показаться, что после входа пользователя в систему проверка подлинности больше не производится. Это впечатление обманчиво, и за кажущейся простотой обращения к ресурсам сети Windows NT скрывается сложный механизм постоянной проверки регистрационной информации о пользователе, срабатывающий каждый раз, когда он пытается получить доступ к ресурсам любого Windows NT-компьютера (и даже компьютера с операционной системой Windows 95, если доступ к его ресурсам контролируется доменом).

Естественно, такая система проверки требует постоянной передачи по сети информации об именах и паролях пользователей. Поэтому для грамотного обеспечения защиты сетей на базе Windows NT необходимо четко представлять процессы, лежащие в основе механизма проверки подлинности пользователей, и то, какая, когда и в каком виде регистрационная информация передается по сети.

### Интерактивный и удаленный вход

Пользователь начинает работу в сети с интерактивного входа: он должен ввести свое имя и пароль, зарегистрированные в базе данных домена. Пользователь, вошедший в домен с Windows NT-компьютера, по завершении проверки подлинности получает из соответствующей базы данных уникальный идентификатор безопасности (SID), однозначно определяющий этого пользователя при работе с ресурсами того компьютера с Windows NT, с которого он вошел в систему. При входе в домен с компьютера с другими операционными системами, такими как Windows 95, пользователю, подлинность которого проверена контроллером домена, разрешается войти в сеть с определенным уровнем полномочий.

Удаленный вход имеет место, когда пользователь уже вошел в систему интерактивно и пытается установить связь по сети с другим Windows NT-компьютером. Это случается, например, при подключения к общему ресурсу через диалоговое окно Map Network Drive или по команде net use, при открытии совместно используемой папки на удаленном компьютере с помощью программы Windows NT Explorer или через диалоговое окно Run. При этом сервер, к которому подключается пользователь, вновь проверяет подлинность, а затем создает для него маркер доступа к ресурсам данного сервера.

### Служба Net Logon

На любом компьютере с Windows NT, входящем в домен, работает служба NetLogon, одна из задач которой — обеспечение проверки подлинности пользователей при входе в домен. На компьютере с Windows NT Workstation или отдельном сервере с Windows NT Server служба Net-Logon принимает запросы на вход с локального компьютера и передает их контроллеру домена. На контроллере домена служба NetLogon обрабатывает эти запросы и передает ответ компьютеру, с которого пользователь входит в домен.

Служба NetLogon отвечает за:

* установление безопасного канала между Windows NT-компьютером, входящим в домен, и контроллером домена, а также между контроллерами доменов, связанных доверительными отношениями;
* сквозную проверку подлинности, т.е. передачу регистрационной информации пользователя на тот контроллер домена, где хранится учетная запись пользователя.

### Обнаружение

Проверка подлинности пользователей в домене — задача контроллеров домена (основного или дополнительных). Поэтому компьютер, с которого пользователь входит в домен, должен сначала найти в сети контроллер домена. Этот процесс называется обнаружением (discovery).

При запуске компьютер с Windows NT пытается обнаружить в сети контроллер своего домена. Если запускается резервный контроллер домена, он пытается обнаружить основной контроллер домена. Наконец, основной контроллер домена должен найти контроллеры всех доверяемых (trusted) доменов.

Клиенты других операционных систем Microsoft проводят обнаружение, только если нужна проверка подлинности пользователей домена.

### Установление безопасного канала

Когда Windows NT-компьютер обнаружит контроллер домена, начинается установление безопасного канала (secure channel). Здесь безопасный канал — это соединение между Windows NT-компьютером и контроллером домена, устанавливаемое, только когда эти два компьютера «знают» друг друга и проверили подлинность каждого. По этому каналу затем передается регистрационная информация о пользователях домена.

Служба NetLogon пытается установить безопасный канал после запуска компьютера и завершения процесса обнаружения, если это не удается, попытки повторяются каждые 15 минут или если возникнет необходимость в проверке подлинности.

### Учетные записи компьютеров и доменов

При установлении безопасного канала службы NetLogon компьютеров с Windows NT посылают друг другу «вызовы» и «ответы», чтобы произвести взаимную проверку подлинности. При этом используются учетные записи домена и зарегистрированных в домене Windows NT-компьютеров. Существует три типа таких записей:

* учетная запись доверия рабочей станции (WORKSTATION\_TRUST\_ ACCOUNT) — для проверки подлинности входящего в домен компьютера с Windows NT Workstation или отдельного сервера с Windows NT Server;
* учетная запись доверия серверу (SERVER\_TRUST\_ACCOUNT) — для проверки подлинности резервных контроллеров домена;
* учетная запись доверия между доменами (INTERDOMAIN\_TRUST\_ACCOUNT) — для проверки подлинности доверительных отношений между доменами Windows NT.

Эти учетные записи хранятся в базе данных SAM в разделе реестра HKEY\_LOCAL\_MACHINE\SAM\SAM\Domains\Account\Users и в базе данных соответствующего Windows NT-компьютера (рабочей станции, резервного контроллера домена или контроллера доверяющего домена) — в разделе реестра HKEY\_LOCAL\_MACHINE\Security\Policy\Secrets.

Учетные записи компьютеров, как и пользователей, включают имя и пароль. Для компьютеров имя учетной записи — это всегда имя компьютера со знаком доллара ($) на конце. Первоначальные пароли учетных записей рабочей станции с операционной системой Windows NT или отдельного сервера в домене устанавливаются такими же, как и имена этих компьютеров (в нижнем регистре и, если нужно, усеченные до 14 символов). Первоначальный пароль для учетной записи доверия между доменами задается в диалоговом окне Add Trusting Domain программы User Manager for Domains при установлении доверительных отношений со стороны доверяемого домена. Эти пароли работают до момента активизации членства соответствующего компьютера с Windows NT в домене или активизации доверительных отношений между доменами, после чего меняются автоматически каждую неделю. Процедуру смены пароля можно отключить как со стороны контроллера домена, так и со стороны рабочей станции.

### Обмен сообщениями при образовании безопасного канала

Обмен сообщениями при образовании безопасного канала происходит следующим образом.

1. Windows NT-компьютер (клиент) устанавливает сеансы TCP/IP и NetBIOS с соответствующим контроллером домена (сервером), способным проверять пользователей при входе в домен.
2. Открывается анонимный доступ к ресурсу IРС$. Для этого сначала согласуется диалект протокола SMB командой SMB\_COM\_NEGO-TIATE. Далее открывается анонимный сеанс SMB, т.е. в запросе SMB\_COM\_SESSION\_SETUP\_ANDX указывается пустое имя пользователя и пароль, и, наконец, командой SMB\_COM\_TREE\_CON-NECT подключается дерево с именем IРС$.
3. Клиент, используя команду SMB\_COM\_CREATE\_ANDX протокола SMB, создает на контроллере домена именованный канал (named pipe) с именем NETLOGON. Передаваемая по нему информация будет обрабатываться службой NetLogon контроллера домена.
4. Используя именованный канал NETLOGON, клиент инициирует установление связи по механизму удаленного вызова процедур (RPC Bind), передавая серверу номера и версии интерфейсов, один из которых — Abstract Interface UUID = 12345678-1234-ABCD-EFOO-01234567CFFB — требуется самому клиенту, а другой — Transfer Interface UUID = 8A885D04-1CEB-11C9-9FE8-08002B104860 — нужен серверу для передачи. Интерфейс представляет собой обозначение некоторой библиотеки процедур, исполнение которых может быть вызвано с удаленного компьютера. Сервер подтверждает существование запрошенного интерфейса. Подтверждение содержит, в частности, имя службы, с которой устанавливается взаимодействие — в данном случае это \PIPE\lsass, т.е. подсистема локального администратора безопасности сервера.
5. Далее идет собственно образование безопасного канала, включающее удаленный вызов двух процедур. Первой клиент вызывает процедуру NetrServerReqChallenge. В качестве параметров в запросе передается имя сервера, с которым устанавливается безопасный канал, имя клиента (в данном случае имя компьютера) и «вызов клиента» — последовательность из 8 случайных байтов. Возвращаемый сервером клиенту результат работы процедуры — «вызов сервера», тоже последовательность из 8 случайных байтов, отличная от «вызова клиента». Используя оба «вызова» и хешированный пароль данного компьютера, и клиент, и сервер вычисляют так называемый ключ сеанса (session key), применяемый впоследствии для проверки подлинности передаваемой по безопасному каналу информации.
6. После этого клиент рассчитывает свой мандат (credentials), дважды шифруя свой «вызов» ключом сеанса по алгоритму DES. Мандат — 8 байтов, призванных доказать серверу, что клиент знает свой «вызов» и ключ сеанса, — посылается как один из параметров при удаленном вызове процедуры NetrServerAuthenticate2. Другие параметры этой процедуры — имена сервера, самого Windows NT-компьютера и его учетной записи в домене.

Если принятая сервером информация совпадает с рассчитанной им самим (напомним, что сервер уже знает и ключ сеанса, и «вызов клиента»), он отвечает клиенту подтверждением успешного выполнения RPC. Одновременно клиенту для проверки подлинности передается мандат сервера, рассчитанный теперь уже на основе «вызова» сервера. Клиент проверяет эту информацию, сравнивая полученные 8 байтов с рассчитанными им самим, и в случае совпадения процедура организации безопасного канала успешно завершается. Важное примечание: мандаты клиента и сервера сохраняются и в дальнейшем служат для проверки подлинности учетных записей как пользователей при их входе в домен, так и Windows NT-компьютеров — например, при смене пароля рабочей станции в домене.

Взаимная проверка подлинности Windows NT-компьютера и контроллера домена — обязательное условие последующего входа пользователей с этого компьютера в домен.

### Сквозная проверка подлинности

Сквозная проверка подлинности (pass-through authentication) происходит, когда компьютер не может идентифицировать пользователя, привлекая свою локальную базу данных учетных записей, а именно:

При интерактивном входе в систему на рабочей станции с Windows NT Workstation или на отдельном сервере Windows NT Server, если в поле Domain диалогового окна Logon Information указано имя домена или доверяемого домена. При этом компьютер по безопасному каналу передает запрос на проверку подлинности контроллеру своего домена. Контроллер проверяет введенное имя домена и, если оно совпадает с именем его собственного, сам проверяет подлинность с помощью своей базы учетных записей и возвращает идентификационную информацию компьютеру входа. Если указанное в поле Domain имя не совпадает с именем домена, к которому он принадлежит, контроллер проверяет, не совпадает ли данное имя с именем доверяемого домена. При совпадении устанавливается безопасный канал с контроллером доверяемого домена, и ему передается запрос на проверку подлинности данного пользователя. Контроллер доверяемого домена обрабатывает этот запрос, сверяя полученную информацию с той, что храниться в его базе данных, и посылает идентификационные данные исходному контроллеру домена, который в свою очередь передает их компьютеру входа. Если учетная запись пользователя не найдена, попытка входа завершается неудачей.

### Вход в домен с Windows NT – компьютеров

Интерактивный вход на компьютере с операционной системой Windows NT начинается после того, как пользователь, нажав комбинацию клавиш Ctrl+Alt+Delete, вызывает диалоговое окно Logon Information и вводит свою регистрационную информацию. При этом в поле Domain выбирается либо имя домена, либо имя доверяемого домена, либо имя компьютера, где зарегистрирован этот пользователь (если компьютер не является членом домена, поле Domain просто не появляется в диалоговом окне Logon Information).

После щелчка кнопки ОК компьютер проверяет имя домена. Если имя, введенное в поле Domain, совпадает с именем компьютера, подлинность пользователя проверяется на основании информации из локальной базы данных. Это просто вход в компьютер с операционной системой Windows NT, а не в домен. Если же имя в поле Domain отличается от имени компьютера, т.е. это имя либо своего, либо доверяемого домена, компьютер входа посылает введенные данные контроллеру своего домена. Контроллер анализирует имя домена, а затем либо сам проверяет подлинность введенной пользователем информации, либо передает ее для проверки контроллеру доверяемого домена.

При удаленном входе в компьютер с Windows NT регистрационная информация о пользователе передается от клиента к серверу по протоколу SMB. Однако если сервер не является контроллером домена, то идет такая же процедура сквозной проверки подлинности, что и при интерактивном входе. Полученные Windows NT-компьютером по протоколу SMB сведения (в частности, зашифрованный с помощью хешированного пароля пользователя «вызов» сервера) передаются между компьютерами Windows NT с помощью запроса RPC NetrLogonSamLogon. При этом дополнительное шифрование ключом, согласованным при установлении безопасного канала, не производится.

### Кэширование информации о пользователе на компьютере с Windows NT

При первом входе пользователя в домен с какого-либо компьютера контроллер домена передает проверенную информацию о нем на компьютер входа. Эта информация кэшируется компьютером в локальном реестре в разделе HKEY\_LOCAL\_MACHINE\SECURITY\Policy\Secrets и в дальнейшем может служить для проверки подлинности пользователей, когда ни один контроллер домена не доступен.

Таким образом, даже если все контроллеры домена выключены, несколько (по умолчанию 10) пользователей, которые последними интерактивно регистрировались в домене с данного компьютера, смогут войти в домен с помощью кэшированных данных. Регистрационная информация о пользователях, входивших в компьютер, а не в домен, также хранится в локальной базе данных этого Windows NT-компьютера.

### Вход в домен с клиентских компьютеров, отличных от Windows NT

Клиентские компьютеры, работающие под управлением Windows 95, Windows for Workgroups, MS-DOS, Macintosh или LAN Manager 2.x, могут взаимодействовать с доменами. Их принципиальное отличие от Windows NT-компьютеров в том, что они не регистрируются в базе данных каталога домена. С точки зрения защиты, эти клиенты заметно уступают клиентам с операционной системой Windows NT и, естественно, представляют собой намного большую угрозу системе безопасности сети.

И все же пользователи этих компьютеров могут иметь учетные записи в базе данных домена. Их вход в домен с клиентских компьютеров управляется контроллером домена.

Компьютеры клиентов не получают регистрационной информации о пользователе, которая могла быть кэширована на рабочей станции и впоследствии задействована для доступа к ресурсам. Поэтому, если при входе с компьютера указанных выше клиентов контроллер домена недоступен, пользователь не сможет работать с сетевыми ресурсами.

Указанные клиенты не имеют возможности выбрать имя доверяемого домена при входе в систему, поскольку такие компьютеры жестко привязаны к определенному домену. Однако эти пользователи могут соединяться с Windows NT-компьютерами как своего, так и других доменов. При этом учетные данные пользователя обрабатываются в таком порядке (до момента успешной регистрации): сначала самим компьютером, затем контроллером домена, к которому компьютер принадлежит, и — при соединении с компьютером доверяющего домена — контроллером доверяемого домена.

### Кэширование паролей на клиентских компьютерах, отличных от Windows NT

Вход в домен Windows NT с компьютеров, управляемых Windows 95, Windows for Workgroups, MS-DOS (c Microsoft Network Client v3.0) и др., требует ввода двух паролей: одного — соответствующей операционной системы и другого — для входа в домен Windows NT. При первом входе запрашиваются оба пароля, а в дальнейшем, если были указаны одинаковые пароли, только первый. По умолчанию информация о всех паролях сохраняется в файле с расширением .PWL, создаваемом для пользователя на локальном компьютере.

Конечно, для пользователей такая система существенно упрощает процедуру входа в домен и другие сети. Однако она заметно ослабляет защищенность сети, поскольку регистрационная информация пользователя домена в момент работы хранится как в памяти клиентского компьютера с такой операционной системой, так и в соответствующем PWL-файле на локальном жестком диске, откуда ее может извлечь злоумышленник.

Для улучшения безопасности сети можно отменить кэширование паролей клиентов такого типа.

### Возможные атаки

#### Перехват пароля при входе программой-имитатором

Одним из способов получения регистрационной информации о пользователе с целью проникновения в сеть является загрузка с дискеты операционной системы MS-DOS и запуск программы, имитирующей поведение операционной системы Windows NT. Задача такой программы — вывести на экран диалоговое окно Logon Information, получить информацию о имени и пароле пользователя, передать ее по сети на компьютер злоумышленника в локальной сети или в Интернете, затем выдать некоторую правдоподобную по диагностике «ошибку», и остановить компьютер. Естественно, после перезагрузки вход в систему протекает нормально, и неопытный пользователь может не заметить подвоха.

#### Перехват и подбор ключа сеанса

Поскольку исходный пароль учетной записи Windows NT-компьютера устанавливается равным имени этого компьютера, злоумышленник, получивший возможность «прослушивать» сеть, может легко рассчитать ключ сеанса. Для этого достаточно перехватить пакеты NetrServerReq-Challenge и определить «вызовы» клиента и сервера. Естественно, после этого злоумышленник может довольно легко определить и новый пароль учетной записи компьютера, и хешированные пароли всех пользователей, входивших в домен до перезагрузки операционной системы.

#### Сканирование паролей в памяти клиентских операционных систем

При наличии в домене клиентов с операционными системами, отличными от Windows NT, пароли шифруются при взаимодействии компьютеров по сети. Однако в памяти компьютера, с которого клиенты входят в сеть, пароли хранятся незашифрованными. Поэтому, зная в деталях внутреннюю структуру памяти такой операционной системы, можно написать программу извлечения пароля пользователя из памяти.

#### Расшифровка паролей, хранящихся в PWL-файлах

Пароль входа в клиентскую операционную систему Windows 95 (исходной версии и версии OSR1), Windows for Workgroups, MS-DOS (c Microsoft Network Client v3.0) служит (после некоторого преобразования) в качестве ключа шифрования PWL-файла данного пользователя по алгоритму RC4. При этом обычно (если не принять дополнительных мер), пароль преобразуется в 32-разрядный ключ, обладающий низкой защищенностью.

#### Атака Man-in-the-Middle

Это атака, работающая в момент проверки подлинности при входе в домен Windows NT. Man-in-the-Middle основана на том, что в пакете NetrLogonSamLogon, передаваемом контроллером домена компьютеру с Windows NT, сведения о группах, членом которых является пользователь, передаются незашифрованными. Поэтому легко обеспечить «прозрачное» изменение информации о членстве входящего в систему пользователя в тех или иных группах, «включив» его таким образом, к примеру, в группу Domain Admins.

## 

## Основные меры защиты. Общие сведения

### 

### Использование только клиентов с Windows NT

В сетях следует избегать установки на клиентских рабочих станциях отличных от Windows NT операционных систем. Как мы видели, только Windows NT-компьютеры имеют свои учетные записи в домене, и, следовательно, вход пользователей в домен с таких компьютеров возможен только при совпадении паролей, хранящихся на локальном компьютере и в домене.

Мы уже говорили, что первоначальный пароль учетной записи любого Windows NT-компьютера хорошо известен. Поэтому, войдя в домен, перезагрузите компьютер.

### Комбинация Ctrl + Alt + Del

Всех пользователей следует проинструктировать, чтобы они обязательно инициировали процедуру входа в систему нажатием комбинации клавиш Ctrl + Alt + Del. Таким способом пользователи смогут нарушить работу программ MS-DOS, имитирующих диалоговое окно Logon Information, и запустить безопасную процедуру регистрации в Windows NT.

### Правила работы для клиентов, отличных от Windows NT

Как уже говорилось, при работе в домене Windows NT для повышения безопасности сети не рекомендуется использовать клиенты Windows 95, Windows for Workgroups или MS-DOS. Если же такая необходимость существует, установите следующие правила работы клиентов:

* Не оставлять компьютер без присмотра после входа в сеть.
* Выходить из системы, если необходимо покинуть компьютер на длительное время, или защититься заставкой с паролем.
* Не запускать на своем компьютере программы, полученные из ненадежных источников в сети, по Интернету или присланные по электронной почте. Такие программы могут просканировать память Вашего компьютера, определить Ваши идентификационные данные и переслать их злоумышленнику.
* Не сохранять пароли пользователя в соответствующих PWL-файлах на локальных компьютерах с операционными системами Windows 95 (исходный выпуск или версия OSR1). Отключить кэширование паролей можно либо с помощью системной политики, либо добавив в раздел реестра HKEY\_LOCAL\_MACHINE\ Software\ Microsoft \ Windows \ CurrentVersion \ Policies \ Network параметр DisablePwdCaching и задав ему значение 1.

Для обеспечения шифрования паролей пользователей Windows NT в памяти клиентских компьютеров с Windows 95 следует установить специальный пакет обновления, исправляющий этот недостаток (программы SecUpd.exe для исходного выпуска Windows 95 или версии OSR1 и SecUpd2.exe для версии OSR2 и OSR2.1 легко найти в Интернете).

### Регулирование входа в систему средствами системной политики

Операционные системы Windows NT и Windows 95 предоставляют администратору сети ряд инструментов регулирования процесса входа пользователей в компьютер с Windows NT или в домен средствами системной политики. Ниже приведены некоторые из них. Установки для клиентов Windows 95 в основном находятся в папке Стандартный компьютер/Сеть.

Этот параметр Делает следующее

Вход в сеть/Заставка для входа в сеть

Вход в сеть/Требовать для входа в Windows проверки пароля сетью

Клиент для сетей Windows/Вход в сеть Windows NT/ Имя домена

Клиент для сетей Windows/ Вход в сеть Windows NT/ Выводить подтверждение входа в домен

Клиент для сетей Windows/ Вход в сеть Windows NT/ Отменить кэширование пароля входа в домен

Пароли/Скрыть пароли для доступа к ресурсам.

Пароли/Отключить кэширование паролей

Пароли/Алфавитно-цифровой пароль для входа в Windows

Пароли/Минимальная длина пароля входа в Windows.

Удаленный доступ к сети/ Запретить удаленный доступ к сети

Устанавливает предупреждающее сообщение при входе пользователей в сеть.

Устанавливает обязательную проверку идентификационной информации пользователя сервером для входа в Windows.

Определяет имя домена Windows NT.

Выводит подтверждение после проверки пользователя контроллером домена.

Отключает кэширование сетевого пароля пользователя в .PWL-файле.

Включает режим замены любых символов символом «\*» при вводе пароля доступа к общему ресурсу. Установка по умолчанию.

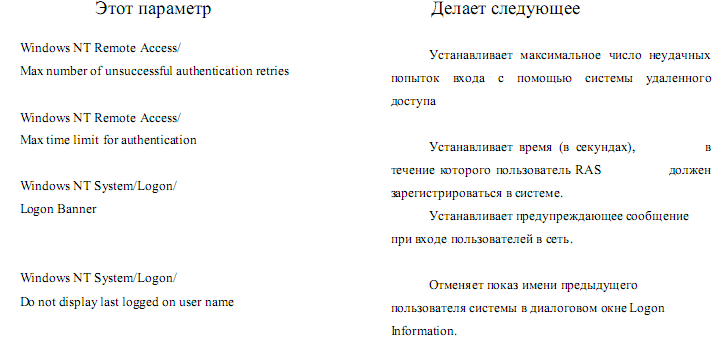
Предотвращает сохранение паролей в PWL-файле. (При этом возможность быстрого входа в сеть для пользователя становится недоступной.)

Устанавливает обязательность наличия в пароле как букв, так и цифр.

Устанавливает минимальную длину пароля для входа в Windows

Отключает возможность соединения с компьютером с помощью службы удаленного доступа.

Правила системной политики для клиентов Windows NT можно найти в папке Default Computer.



Применяя эти правила, можно значительно повысить уровень безопасности сети на базе домена Windows NT.

## Рекомендации

Для сети с количеством машин более 10 обязательно наличие резервного контролера домена Windows NT.

В соответствии с политикой безопасности предприятия рекомендуется создать в домене Windows NT глобальные группы пользователей.

На системах с машинами Windows 95 / 98 следует включить вход в домен Windows NT и разграничение доступа на уровне пользователей.

Обязательно следует разработать файлы системных политик для Windows 95 и Windows NT. Напомним, файл системных политик для Windows 95 называется Config.pol, а для Windows NT – NTConfig.pol. Эти файлы должны размещаться в директории NetLogon контроллеров домена. Форматы этих файлов отличаются, причем редакторы политик могут запускаться только на машине с соответствующей операционной системой.

В этих файлах следует как минимум установить параметры, запрещающие запись паролей в файлах .PWL, число попыток входа в систему и т.п. (см. предыдущий раздел).

Локальный вход на контроллер домена должен быть разрешен только администраторам и операторам резервного копирования.

Следует по возможности в качестве ОС клиентских машин использовать Windows NT Workstation с последним Service Pack’ом. Не рекомендуется использовать Windows 95, Windows 98 защищена лучше.

Следует внимательно следить за количеством расшаренных ресурсов и правами на доступ к ним.

Разделы ОС Windows NT рекомендуется форматировать с использованием файловой системы NTFS (для удобства, хоть это и понижает безопасность, рекомендуется в качестве первого раздела иметь небольшой (~200 Mb) раздел FAT16). При использовании данной файловой системы следует внимательно устанавливать разрешения (Permissions) на доступ к файлам.

Для домашних директорий пользователей следует устанавливать разрешения Full Control для администраторов и Change для пользователя. Вообще, где это возможно, следует вместо разрешения Full Control давать разрешение Change, которое позволяет считывать и записывать информацию, но не позволяет стать владельцем и изменить Permissions.

Особо важную информацию не стоит хранить на локальных компьютерах. Лучше создать на разделе NTFS расшаренный ресурс и дать к нему доступ ограниченному кругу лиц. Следует иметь в виду, что папки и файлы, создаваемые на рабочем столе, при входе пользователя в сеть, как и весь профиль, копируются на локальный компьютер, поэтому лучше создавать их на сетевом домашнем диске пользователя. Особенно это актуально для Windows 95 / 98, так как файловые системы FAT16 и FAT32 не позволяют ограничить к ним доступ. Это важно при наличии у пользователя сетевого домашнего каталога. В особо важных случаях можно с помощью редактора системных политик задать полные пути к файлам профиля, в том числе и сетевые.

Для затруднения взлома системы встроенную учетную запись администратора следует переименовать и создать новую учетную запись с именем Administrator (Администратор для русской версии NT) с минимальными правами.

Наиболее распространенной ошибкой является постоянная работа с администраторскими правами. Повседневные действия следует выполнять, работая под аккаунтом обычного пользователя, с администраторскими правами – только в случае необходимости. При работе с администраторскими правами следует быть внимательным и не запускать подозрительные и незнакомые файлы, т.к. в этом случае программа сразу приобретает едва ли не полный доступ ко всем ресурсам компьютера.

Большую опасность, особенно для систем Windows 95 / 98 играют вирусы. Обязательно следует на каждый компьютер установить антивирусный пакет (например, AVP лаборатории Касперского) и периодически обновлять его антивирусную БД.

Крайне не рекомендуется для исполняемых файлов давать право доступа Write пользователям, которым такое право не нужно. Обычно достаточно оставить его администраторам, а для остальных пользователей – право читать и выполнять их.

Хороший системный администратор должен несколько раз в сутки просматривать системный журнал контроллера домена и серверов. При большом количестве журналов можно поискать в Интернете и установить специальные средства чтения и объединения системных журналов нескольких компьютеров Windows NT в одну БД.

Рекомендуется разрешать пользователям применять алфавитно-цифровые пароли длинной не менее 7 символов и помнить 5 последних паролей. Автоматическую смену паролей рекомендуется ставить каждые 45 дней.

Для проверки паролей пользователей на стойкость рекомендуется использовать программу L0phtCrack, запустив которую на контроллере домена с администраторскими правами, можно выяснить, насколько быстро открываются пароли пользователей.

Рекомендуется как можно раньше устанавливать на используемые программные продукты так называемые заплатки (hotfix) и Service Pack’и. Информацию о них обычно можно получить с WWW-сайта производителя (например, www.microsoft.com).

Если вы хотите быть в курсе последних обнаруженных “дыр” в системе Windows NT, а также получать другую, относящуюся к безопасности NT информацию, вы можете подписаться на список рассылки NTBugTraq (www.ntbugtraq.com).

Чтобы построить действительно защищенную систему, необходимо каждый день просматривать этот и ему подобные списки рассылки и, узнав об обнаруженных уязвимостях, своевременно на них реагировать.

# Безопасность Microsoft Proxy Server 2.0

## 

## Общий обзор — сети, безопасность, производительность и цены

### Проблемы безопасности, производительности и цен

Среди наиболее серьезных факторов, препятствующих подключению внутренних сетей организаций любого масштаба к Интернету, нельзя не назвать проблемы обеспечения безопасности, управляемости и цены. Для их эффективного решения и предназначены брандмауэры и серверы кэширования информации.

### Брандмауэры обеспечивают безопасность

Большинство людей знакомо с термином "брандмауэр". Он широко распространен и вполне обоснованно применяется для обозначения аппаратного или программного обеспечения, которое используется для ограничения возможностей доступа в корпоративную сеть организации из Интернета. Как правило, брандмауэры реализуют защиту на нескольких уровнях — обычно, на транспортном и сетевом уровнях. Однако, нередко брандмауэрами называют и маршрутизаторы, имеющие лишь функцию фильтрации пакетов. Кроме того, брандмауэр обычно предоставляет некоторый механизм уведомления сетевого администратора о происходящей “атаке” или “вторжении”. Некоторые продукты этой группы поддерживают также организацию виртуальных частных сетей (virtual private networks, VPN), соединяющих географически разделенные сегменты. Применение VPN позволяет реализовать недорогое защищенное соединение, например, между офисом филиала и главной штаб-квартирой корпорации по общедоступной коммуникационной инфраструктуре.

### Кэширование информации способствует повышению производительности сети и сокращению затрат

Если брандмауэры обеспечивают безопасность, то серверы кэширования и прокси-серверы — повышение производительности сети и снижение издержек. Благодаря кэшированию потребности пользователей удается удовлетворить, не передавая данные на большие расстояния по общедоступному Интернету или по корпоративной сети. В результате сокращается сетевой трафик и уменьшается коэффициент загрузки сети. В дополнение к этому, многие прокси-серверы позволяют сетевым администраторам указывать, с какими из служб Интернета могут работать их пользователи. Эти возможности называют контролем доступа пользователей и фильтрацией сервисов.

Кэширование информации уже давно играет важную роль в работе многих крупных предприятий и компаний - поставщиков Интернет-услуг (Internet Service Provider, ISP). Сегодня эта технология прокладывает себе путь в вычислительные системы менее крупных организаций, а в будущем кэширование информации, очевидно, станет важнейшей функцией для компаний любого масштаба. Все более широкое применение Интернет-технологий для построения корпоративных интрасетей и внедрение в практику push-систем, которые обеспечивают заблаговременную доставку информации по Интернету или интрасети на рабочее место пользователя, приведут, по-видимому, к дополнительному увеличению спроса на прокси-серверы.

### Что такое “прокси-сервер”?

Proxy переводится на русский язык как "выполняющий чье-то поручение". Прокси-сервер в рамках сетевой терминологии обозначает компьютер, который обслуживает несколько клиентских ПК, обращающихся с запросами к Интернету или к каким-либо ресурсам в пределах корпоративной интрасети. Прокси-сервер представляет собой защищенный шлюз между Интернетом / интрасетью и этими клиентскими ПК.

Прокси-сервер остается более или менее прозрачным для остальных участников коммуникационного процесса — пользователя и источника информации в Интернете. Пользователь, осуществляющий доступ к Интернету со своего настольного компьютера, не должен замечать присутствия прокси-сервера между ним и Всемирной сетью помимо тех случаев, когда он пытается обратиться к службе или к узлу Интернета, доступ к которым ему закрыт. А для Web-сервера, получающего по Интернету запросы от прокси-сервера, они должны быть неотличимы от запросов, полученных непосредственно от средства просмотра Web-ресурсов или FTP-клиента.

Описанный сценарий требует, чтобы прокси-сервер был двусторонним, то есть компьютер, на котором он работает, должен быть оснащен двумя сетевыми интерфейсами: один для подключения к сети предприятия, а второй — для связи с внешним миром, в данном случае — с Интернетом

## Общий обзор Microsoft Proxy Server 2.0

Microsoft Proxy Server 2.0 представляет собой брандмауэр с расширяемым набором функций и сервер кэширования информации, применение которого на предприятии любых масштабов позволяет повысить безопасность доступа к Интернету, а также сократить время отклика и повысить эффективность функционирования сети в среднем на 50%.

Microsoft Proxy Server входит в состав семейства серверных приложений Microsoft BackOffice®.

Microsoft Proxy Server выполняет опережающее кэширование ресурсов, к которым пользователи обращаются чаще всего, обеспечивая их постоянную актуальность и доступность. Данные автоматически заблаговременно загружаются из сети и обновляются на основе эвристических алгоритмов, учитывающих статистику обращений.

### Расширяемость набора функций обеспечения безопасности

В дополнение к защите на уровне приложений и защите на уровне коммуникационных каналов этот продукт поддерживает динамическую фильтрацию пакетов. Он дополнен также функциями выдачи предупреждающих уведомлений и ведения регистрационного журнала, которые необходимы пользователям брандмауэров. Сверх того, совместное использование Microsoft Proxy Server с модернизированной службой Routing and Remote Access Service ОС Windows NT Server позволяет реализовать экономичные и защищенные виртуальные частные сети (Virtual Private Network, VPN).

Microsoft Proxy Server может играть важную роль в комплексной стратегии обеспечения безопасности информационной системы организации. Пользователям предлагается широкий выбор фильтров для защиты от вирусов и вредоносных программных компонентов, основанных на технологиях Java и ActiveX™, средств блокировки доступа к нежелательным узлам, а также других средств защиты, производимых независимыми компаниями и опирающихся на платформу Microsoft Proxy Server.

## Задачи прокси-сервера типовой сети

MS Proxy Server, используемый в нашей типовой сети, должен выполнять следующие функции:

* служить шлюзом между внутренней сетью организации и сетью Интернет. Т.о., организации для подключения к Интернету можно не получать от провайдера блок IP-адресов, а достаточно всего одного адреса;
* выполнять функции Web Proxy, в том числе кэшировать информацию, запрашиваемую пользователями внутренней сети по протоколу HTTP;
* выполнять функции WinSock Proxy и Socks Proxy, обеспечивая прозрачный доступ в Интернет для приложений, работающих под управлением ОС Windows и приложений, поддерживающих протокол Socks;
* разграничивать доступ в Интернет на уровне пользователей, используя список пользователей и групп Windows NT (Web Proxy, WinSock Proxy);
* разграничивать доступ в Интернет на уровне компьютеров (Sock Proxy);
* выполнять динамическую фильтрацию TCP, UDP и IP-пакетов, контролируя трафик различных служб в направлении внутренней сети и наоборот (брандмауэр);
* служить шлюзом для доступа к серверам внутренней сети из сети Интернет по таким протоколам, как SMTP, POP3, HTTP.

## 

## Установка и настройка прокси-сервера

### 

### Установка прокси-сервера

MS Proxy Server 2.0 должен устанавливаться на компьютер, работающий под управлением Windows NT 4.0 Server с установленным MS Internet Information Server и Service Pack 3 или выше.

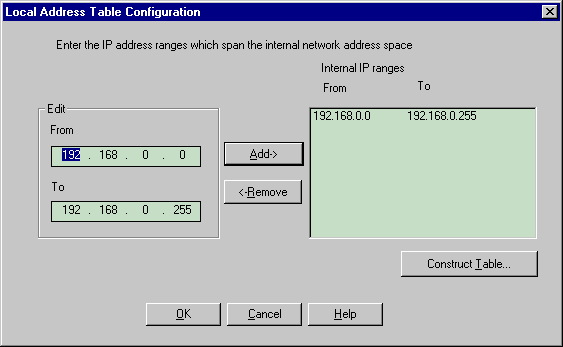
Перед установкой необходимо знать IP-адреса внутренней сети и IP-адрес внешнего интерфейса компьютера, на который устанавливается прокси-сервер.

Т.к. WebProxy для кэширования может использовать только раздел жесткого диска с файловой системой NTFS, на жестком диске должен быть как минимум один такой раздел.

### Настройка таблицы локальных адресов

Таблица локальных адресов (LAT – Local Address Table) используется прокси-сервером для определения того, какие IP-адреса принадлежат внутренней сети организации, а какие – внешней (Интернету). Ее необходимо составлять тщательно и без ошибок, т.к. если в эту таблицу попадут адреса, на самом деле принадлежащие внешней сети, к ним не будут применяться правила фильтрации пакетов, и злоумышленник, работающий с этих адресов, фактически будет приравнен в правах к пользователям внутренней сети. По этой же причине необходимо тщательно отслеживать все изменения LAT.

Для изменения LAT необходимо в свойствах любой из служб прокси нажать кнопку Local Address Table… При этом откроется окно следующего вида:



В поле Edit задаются начальный и конечный IP-адреса диапазона внутренних IP-адресов. В правой части собственно и показана LAT.

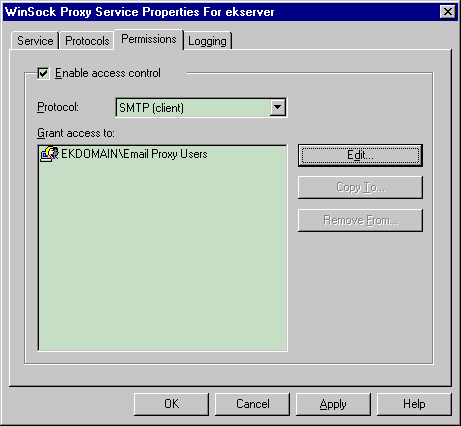
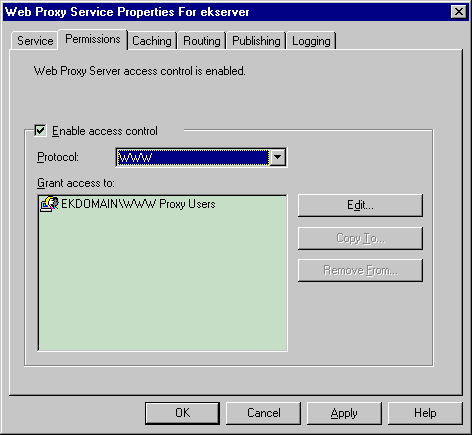
Нажатие кнопки Construct Table открывает окно, в котором можно задать параметры для автоматической конфигурации LAT. Делать это рекомендуется только в том случае, когда точно неизвестны IP-адреса, принадлежащие внутренней сети.

Для нашей типовой сети рекомендуется диапазон 192.168.0.0 – 192.168.0.255, – адреса, выделенные для сетей, которые не подключаются к Интернет напрямую.

### Настройка разрешений пользователям и группам

В соответствии с политикой безопасности организации отдельным пользователям может быть разрешен полный доступ в Интернет, отдельным – доступ только к FTP ресурсам, или, например, электронной почте. MS Proxy Server 2.0 тесно интегрирован с системой безопасности Windows NT и может использовать список пользователей и групп для разрешения им доступа в Интернет по различным протоколам.

Рекомендуется завести отдельные локальные группы для пользователей различных протоколов, например – «Users of FTP Proxy», «Users of WWW Proxy» и т.п. Далее, в настройках Permissions службы Web Proxy или WinSock Proxy нужно дать каждой группе право пользования соответствующим протоколом. Теперь, чтобы дать конкретному пользователю право работать по данному протоколу, достаточно просто включить его в соответствующую группу. И наоборот, чтобы запретить использование протокола – удалить его из группы.



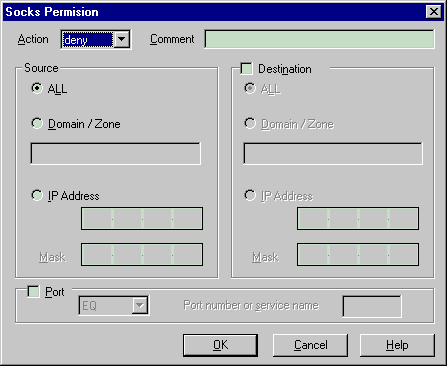
Чтобы включить контроль доступа, необходимо на вкладке Permissions соответствующей службы Proxy (Web Proxy или WinSock Proxy) поставить галочку в поле Enable access control. Кнопка Edit позволяет редактировать список пользователей, которым разрешен доступ к данному протоколу.

Для аутентификации пользователя могут применяться протоколы Basic и Windows NT Challenge / Response. Задать использование протокола можно в свойствах службы WWW.

Протокол аутентификации Basic плох тем, что пароль в нем по сети передается в открытом, т.е. не зашифрованном, виде. В отличие от Basic, протокол Windows NT Challenge / Response всегда передает пароль только в зашифрованном виде. Его преимуществом также является то, что пользователю при доступе не нужно вводить имя / пароль – используются значения, указанные им при входе в сеть. Но этот протокол поддерживается только Microsoft Internet Explorer 2.0 и выше. Т.о., если во внутренней сети функционируют приложения, не поддерживающие Windows NT Challenge / Response, и необходимо ограничить отдельным пользователям доступ в Интернет, единственным выходом остается использование протокола Basic.

В случае, если разрешен анонимный доступ, то пользователи, не указывающие имя / пароль, олицетворяются аккаунтом, указанном в поле Anonymous Logon. Этот тип доступа включать не рекомендуется.

Служба Socks Proxy не поддерживает аутентификацию на уровне пользователей. Для этой службы можно задать фильтр, в котором присутствуют адрес источника, приемника и номер порта.



В поле Action выбирается deny (запретить) или permit (разрешить). В качестве параметров для фильтра указываются:

* в поле Source (отправитель) и Destination (получатель): ALL – все компьютеры; Domain / Zone – домен или зона, указываемая в форме полного доменного имени (например, mycompany.com); IP Address – конкретный IP-адрес с маской подсети;
* в поле Port: операция над номером порта (EQ – равно, NEQ – не равно, GT – больше, LT – меньше, GE – больше или равно, LE – меньше или равно). В поле Port number or service name – номер порта или название службы TCP/IP, с которым происходит сравнение при выполнении указанной операции.
* Порт и получатель учитываются только, если поставить соответствующие галочки.

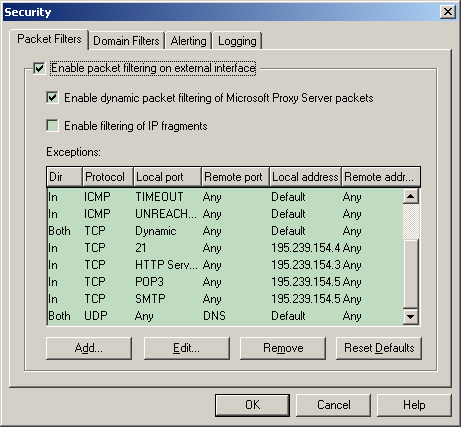
Т.о., для протокола Socks можно запретить доступ к определенным службам отдельным компьютерам. Вообще, если в сети все клиенты работают под управлением MS Windows, то применять протокол Socks не рекомендуется, – его вполне заменяет WinSock.

Для нашей типовой сети рекомендуется следующая политика разграничения доступа:

* служба Socks Proxy отключена;
* включена аутентификация с помощью протокола Windows NT Challenge / Response, аутентификация с помощью протокола Basic отключена, анонимный доступ также отключен;
* для служб Web Proxy и WinSock Proxy включен контроль доступа;
* созданы глобальные группы “Users of Proxy – unlimited”, “Users of WWW Proxy”, “Users of FTP Proxy”, “Users of Gopher Proxy”, “Users of SSL Proxy”, “Users of Email”, “Users of News” и т.п.;
* для Web Proxy разрешен доступ соответствующим группам по четырем поддерживаемым службой протоколам;
* для WinSock Proxy соответствующим группам разрешен доступ к соответствующим протоколам;
* группе “Users of Proxy – unlimited” разрешен доступ ко всем протоколам Web Proxy и Unlimited Access для WinSock Proxy. В эту группу рекомендуется включать только администраторов и руководителей;
* в службе WinSock Proxy доступ к протоколу DNS разрешен группе “Everyone”.

### Настройка фильтрации пакетов

Окно настройки открывается нажатием кнопки Security в свойствах любой из служб прокси и выбором вкладки Packet Filters.



Как принято во всех брандмауэрах, прохождение всех пакетов данных по умолчанию запрещено. Чтобы разрешить прохождение определенных пакетов, надо явно задать для него правило в списке исключений.

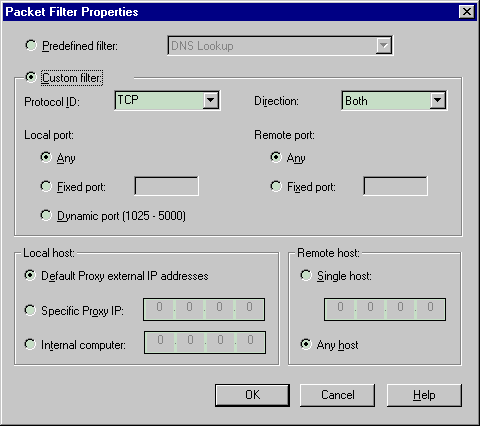
Фильтрация пакетов включается установкой галочки в поле Enable packet filtering for external interface.

Поле Enable dynamic packet filtering of Microsoft Proxy Server packets позволяет включить создание динамических фильтров для соединений, открываемых одной из служб прокси. Если отключить эту возможность, то нужно очень тщательно создавать фильтры вручную.

Поле Enable filtering of IP fragments позволяет включить контроль над фрагментами датаграмм и пакетов данных.

В поле Exceptions собственно и находится список фильтров.

В Microsoft Proxy Server имеется большое количество встроенных фильтров, которые можно добавить кнопкой Add… Также можно создавать пользовательские фильтры.



Параметры фильтра включают в себя протокол (ICMP, TCP, UDP), направление (In, Out, Both), номер локального порта, номер удаленного порта, IP-адрес локального хоста, IP-адрес удаленного хоста. Таким образом, IP-пакет пропускается только в том случае, если его параметры удовлетворяют указанному в одном из фильтров.

Рекомендуется установить следующие настройки:

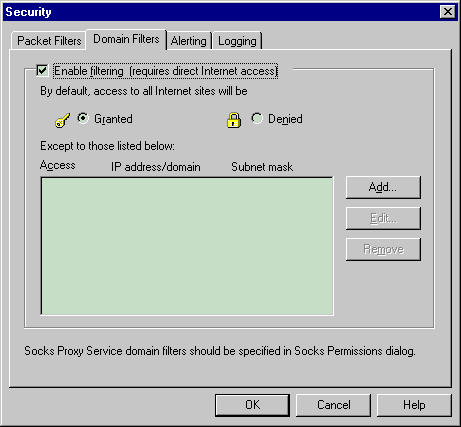
* включить динамическое создание фильтров;
* отключить фильтрацию IP-фрагментов (так как это увеличивает нагрузку на прокси-сервер);
* в дополнение к фильтрам по умолчанию установить фильтры из таблицы 1, которые разрешают доступ к внутренним Web и Mail серверам.

### Таблица 1. Настройка доступа к отдельным узлам и доменам Интернета

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Dir | Protocol | Local port | Remote port | Local address | Remote address |
| Both | TCP | Dynamic | Any | Default | Any |
| In | TCP | 21 | Any | Default | Any |
| In | TCP | HTTP Server (port 80) | Any | Default | Any |
| In | TCP | POP3 | Any | Default | Any |
| In | TCP | SMTP | Any | Default | Any |

### 

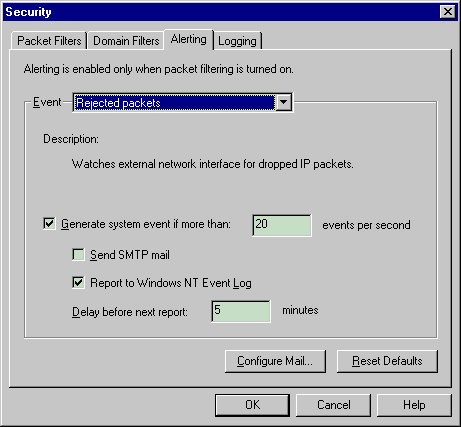
Окно настройки открывается нажатием кнопки Security в свойствах любой из служб прокси и выбором вкладки Domain Filters.



Здесь можно ограничить доступ к конкретным узлам и доменам Интернета в соответствии с политикой организации.

### Настройка генерации предупреждений

Окно настройки открывается нажатием кнопки Security в свойствах любой из служб прокси и выбором вкладки Alerting.



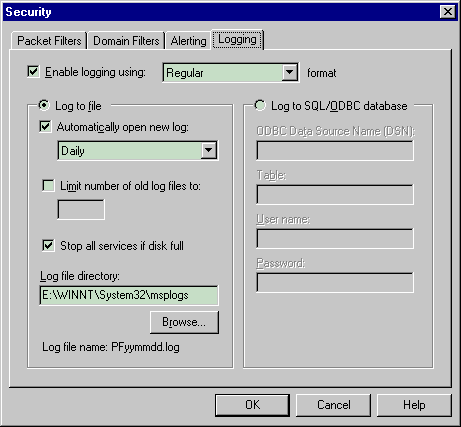
На этой вкладке можно настроить генерацию предупреждений (Alerts) на три типа событий: Rejected Packets (отброшенные пакеты), Protocol violations (выявление в отброшенных пакетах потенциально опасных), Disk full (диск заполнен).

Основанием для генерации предупреждения становится появление события не реже заданного количества раз в секунду.

Рекомендуется оставить настройки по умолчанию. Системному администратору рекомендуется не реже одного раза в сутки просматривать журнал событий Windows NT компьютера, выполняющего функции прокси-сервера.

### Настройка ведения лог-файлов

Окно настройки открывается нажатием кнопки Security в свойствах любой из служб прокси и выбором вкладки Logging.



Лог можно в обычном (Regular) и подробном (Verbose) формате.

Рекомендуется оставить настройки по умолчанию. Системному администратору рекомендуется раз в сутки просматривать сгенерированный за прошедшие сутки лог-файл.

Безопасность Microsoft Exchange Server 5.5

## 

## Общая информация

Microsoft Exchange Server предоставляет решения для организаций в области обмена сообщениями и совместного использования информации. Серверная часть Microsoft Exchange включает службу каталога, хранилище информации, агента передачи сообщений, коннекторы. Все эти компоненты запускаются как Microsoft Windows NT сервисы и работают совместно, обеспечивая следующие возможности:

* управление службой каталога Microsoft Exchange Server;
* управление доступом к информации;
* предоставление структурированного архива документов и электронных сообщений;
* передачу и маршрутизацию сообщений - внутри и за пределы организации;
* контроль за состоянием серверов и соединений;
* синхронизацию каталогов на всех серверах во всех отделениях;
* управление репликацией и разрешение конфликтов репликации.

### Административная программа

Программа Microsoft Exchange Administrator позволяет администраторам с одного места конфигурировать и управлять всей корпоративной системой - почтовыми ящиками пользователей, шлюзами и серверами, находящимися в любом филиале корпорации. Эта программа дает графическое представление всех компонентов системы в виде иерархической структуры, упрощая выполнение основных операций над группой ресурсов на каждом уровне структуры.

### Каталог

Каталог, или адресная книга, Microsoft Exchange Server хранит всю доступную информацию о пользователях и ресурсах организации, включая почтовые ящики, списки рассылки, общие папки, серверы и т.д. Каталог автоматически распространяется на все серверы внутри отделения (Site) и может быть специально настроен для автоматической синхронизации с почтовыми отделениями на других серверах.

Каталог Microsoft Exchange гораздо больше, чем просто адресная книга. В нем может храниться полная информация о пользователях - адрес, телефон, должность и т.д., то есть каталог может использоваться как, например, телефонный справочник организации.

### Хранилище информации

Хранилище информации Microsoft Exchange представляет собой структурированный архив для хранения информации, созданной пользователями. Это нереляционная база данных, разработанная для хранения разнородной информации (такой, как электронная почта, файлы вложений, графика, звук, видео), которая предоставляет быстрый доступ к этим данным. Администраторы имеют возможность:

* устанавливать ограничения на размер хранимых общих и личных папок;
* устанавливать временной лимит и автоматически удалять из хранилища устаревшую информацию;
* определять права доступа к общим папкам;
* тиражировать общие папки по заданному расписанию.

Хранилище информации состоит из двух баз данных: одна используется для хранения личных папок пользователя, другая - для общих папок. Механизм репликаций позволяет автоматически распространять информацию, хранимую в общих папках, на любые серверы Microsoft Exchange.

Личные папки хранят информацию, принадлежащую отдельным пользователям. Только владельцы этих папок могут делегировать права доступа к информации, хранимой в этих папках. Личные папки хранятся в компьютере, на котором установлен Microsoft Exchange Server, и управляются владельцем этой папки.

Общие папки являются ключевым компонентом Microsoft Exchange Server. Благодаря возможности тиражирования этих папок, пользователи имеют доступ к одной и той же информации, независимо от их местонахождения.

Администратор имеет множество средств управления процессом тиражирования. Он может, например, установить различные параметры: время, когда начинается тиражирование, какая информация должна распространяться по организации и т.д.

### Агент передачи сообщений

Агент передачи сообщений (Message Transfer Agent - MTA) служит для маршрутизации и передачи данных на другие серверы и почтовые системы. Это - основа коммуникационной инфраструктуры Microsoft Exchange Server.

Агент передачи сообщений использует четыре компонента для передачи данных:

1. Site коннектор;
2. RAS (Remote Access Service) коннектор;
3. X.400 коннектор;
4. Internet Mail Connector;
5. Newsfeed.

Site коннектор -наиболее эффективный путь для соединения двух отделений (Sites, а точнее - двух MS Exchange серверов), легко настраиваемый и использующий любые сетевые протоколы. Однако для его применения требуется постоянное соединение с высокой скоростью, то есть соединение по сети или выделенный канал. RAS (Remote Access Service) коннектор - частный случай Site коннектора. Но вместо постоянного соединения для его настройки используется сервис удаленного доступа, то есть связь по асинхронным (телефонным) линиям. Такая связь может устанавливается по заданному расписанию.

X.400 коннектор соответствует стандартам X.400 Международного комитета по телефонии и телеграфии (МКТТ), опубликованным в 1984 и 1988 году. Обычно используется, когда необходима передача сообщений в общественные X.400 системы.

Internet Mail Connector позволяет пользователям обмениваться сообщениями с пользователями Internet. Internet Mail Connector поддерживает протоколы SMTP, POP3, IMAP4. Newsfeed – служба, поддерживающая протокол обмена новостями с сетью USENET по протоколу NNTP.

Internet Mail Connector также поддерживает стандарт Internet, известный как MIME (Multipurpose Internet Mail Extension), для передачи мультимедийных объектов, включая текстовые документы, PostScript\* и бинарные файлы, графику, видео, голосовые сообщения и др. Кроме того, Internet Mail Connector поддерживает стандарты для передачи бинарных файлов вложений (Аttachments), использующих UUENCODE.

Internet Mail Connector можно настроить как SMTP клиент, как SMTP сервер или как и клиент, и сервер одновременно. Как сервер, он ожидает соединения с хостом SMTP для принятия сообщений. А как клиент, он инициирует связь с хостом SMTP для отправки исходящих сообщений.

Internet Mail Connector может функционировать как SMTP хост, выполняя маршрутизацию передачи сообщений. Он обращается к серверу имен домена (Domain Name Server) или локальному хосту для того, чтобы определить, куда сообщение должно быть доставлено. Если получатель находится в другой SMTP системе, то Internet Mail Connector или доставит сообщение на искомый SMTP хост, или перешлет на другой SMTP хост для дальнейшей маршрутизации.

## 

## Настройка MS Exchange Server 5.5

### 

### Установка MS Exchange Server 5.5

Инсталляция MS Exchange Server 5.5 достаточно проста и понятна.

В рассматриваемой нами организации в качестве Web-сервера и Mail-сервера физически используется один и тот же компьютер, поскольку при небольшом количестве пользователей (менее 300) ресурсов одного компьютера (Celeron 300, 128 Мб ОЗУ) вполне хватит.

Следует заметить, что службы MS Exchange Server запускаются под одним определенным аккаунтом. Рекомендуется создать специальную учетную запись (например, “ExchAdmin”), которую следует включить в группу “Users of Email”, а из остальных групп исключить. Обязательно нужно убрать у данной учетной записи право Log on locally и установить галочки в полях User cannot change password и Password never expired. Кроме того, этому пользователю следует дать право (Permission) Change на директорию, куда был проинсталлирован Exchange Server. Инсталлировать нужно MS Exchange Server под администраторским аккаунтом, а в качестве аккаунта, под которым будут запускаться службы MS Exchange Server, следует указать вновь созданный (“ExchAdmin”).

### Конфигурирование MS Exchange Server для работы с MS Proxy Server

Как видно из рисунка 1, MS Exchange Server находится в локальной сети и взаимодействует с сетью Интернет через прокси-сервер. Такая схема рекомендуется для повышения уровня защищенности, так как злоумышленнику в данном случае непосредственно почтовый сервер недоступен.

Для работы MS Exchange Server через MS Proxy Server, необходимо, чтобы на компьютере, на котором инсталлирован MS Exchange Server, был также инсталлирован WinSock Proxy Client.

Чтобы привязать порты почтового сервера к внешнему интерфейсу прокси-сервера, необходимо в директории, где расположен файл Msexcimc.exe (это служба, обслуживающая протокол SMTP), создать текстовый файл Wspcfg.ini, содержимое которого приведено ниже:

[Msexcimc]

ServerBindTcpPorts=25

Persistent=1

KillOldSession=1

Также в директории, где расположен файл Store.exe (служба, обслуживающая протоколы POP3, NNTP, IMAP4), необходимо создать второй файл Wspcfg.ini:

[Store]

ServerBindTcpPorts=110,119,143

Persistent=1

KillOldSession=1

В сетевых настройках компьютера, на котором работает Exchange Server, должны быть обязательно прописаны DNS-сервер и домен.

Обычно компании такого масштаба не содержат DNS-сервера для своей зоны. Поэтому в дальнейшем мы учитываем, что за зону компании отвечает провайдер.

Следует обратить особое внимание, что в DNS-сервере, который отвечает за зону нашей типовой организации, в качестве почтового сервера домена должны быть указаны имя и IP-адрес внешнего интерфейса прокси-сервера. Ниже приведены примеры для двух записей, которые обязательно должны быть в DNS-сервере зоны mycompany.com, чтобы можно было использовать почтовые Интернет-адреса типа user@mycompany.com:

@ IN MX 10 proxy

proxy IN A 195.195.195.195

### 

### Общие настройки Exchange Server’а

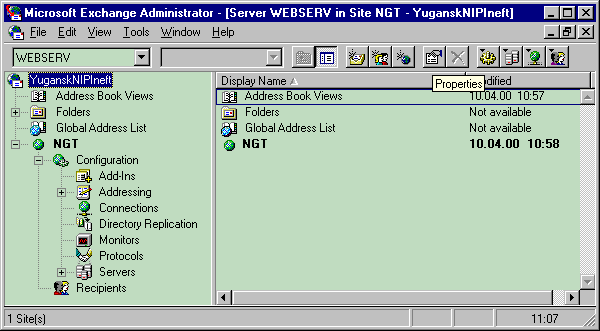
Предполагается, что организация использует только один Exchange Server и нет необходимости организовывать обмен информацией между несколькими почтовыми серверами. Также предполагается, что в сети используются только протоколы Интернет (SMTP, POP3, IMAP4, NNTP).

Так как при первоначальной установке Internet Mail Connector и Newsfeed не устанавливаются, их необходимо установить вручную. Делается это пунктами меню File -> New Other -> Internet Mail Service… и File -> New Other -> Newsfeed…

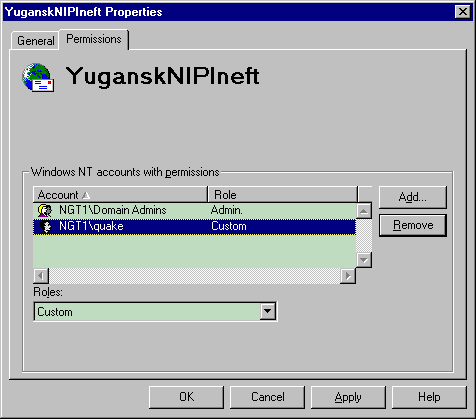
Рекомендуется удалить все неиспользуемые коннекторы, оставив только Internet Mail Connector и Newsfeed (если предполагается предоставлять клиентам возможность работы с новостями USENET).

Крайне рекомендуется установить Service Pack 3 для MS Exchange Server 5.5 (http://www.microsoft.com/exchange/DeployAdmin/sp3.htm). К сожалению, он не распространяется свободно (во всяком случае, на 10.04.2000), поэтому следует установить хотя бы Service Pack 2 (ftp://ftp.microsoft.com/bussys/exchange/exchange-public/fixes/Eng/Exchg5.5/SP2).

Для редактирования списка администраторов почтового сервера организации, необходимо установить выделить самый старший элемент дерева (это и есть организация) и нажать кнопку «Properties» (см. рис).



В появившемся окне следует выбрать вкладку Permissions:



Как и для остальных продуктов, не следует давать администраторские права без необходимости. В рассматриваемой нами организации с администраторскими обязанностями вполне справятся 1-2 человека.

Не рекомендуется заводить почтовые ящики, ассоциированные с администраторскими учетными записями, особенно если к почтовому серверу разрешен доступ по протоколу POP3. Дело в том, что пароль при использовании этого протокола передается по сети в открытом виде, и злоумышленник может перехватить его. Кроме того, он может попытать подобрать его. Как рассматривалось выше, администратор должен работать под учетной записью с правами обычного пользователя, а под администраторским аккаунтом – только в случае необходимости.

В том случае, если администратор по необходимости работает в основном с правами администратора, рекомендуется завести для него учетную запись, которая будет включена только в группу “Users of Email” и завести почтовый ящик, ассоциированный с этой учетной записью. Теперь администратор в качестве почтового ящика может использовать этот почтовый ящик.

### Настройки Internet Mail Connector (Internet Mail Service)

Ниже будут рассмотрены вкладки, играющие роль с точки зрения защиты.

Connections



В поле Accept Connections можно задать условия, при которых сервер будет SMTP-устанавливать соединение с клиентом. From any host – от любого хоста; Only from hosts using Authentication / Encryption / Auth and Encrypt – устанавливать соединение только с хостами, использующими аутентификацию / шифрование / аутентификацию и шифрование. Здесь имеется в виду, что при отправке письма пользователь должен быть авторизован или (и) использовать шифрование. Кнопка Specify by host позволяет указать конкретные компьютеры, от которых ожидается аутентификация / шифрование.

Расположенные ниже поля Clients can only submit if homed on this server и Clients can only submit if authentication account matches submission address позволяет усилить защиту, принимая соединения соответственно только от клиентов, которые имеют на сервере почтовый ящик и от клиентов, параметры аутентификации которых совпадают с параметрами аутентификации пользователя, указанного в поле From (т.е. клиент должен отправлять письмо только от своего имени).

К сожалению, в MS Exchange Server невозможно реализовать обычную схему запрета релеинга (relaying) почты, в соответствии с которой сервер принимает и отправляет почту только в том случае, если пользователь, указанные в поле From или To имеет на нем почтовый ящик. При использовании такой схемы от клиента не требуется аутентификация, а использование почтового сервера для посторонних организаций - рассыльщиков спама становится невозможным.

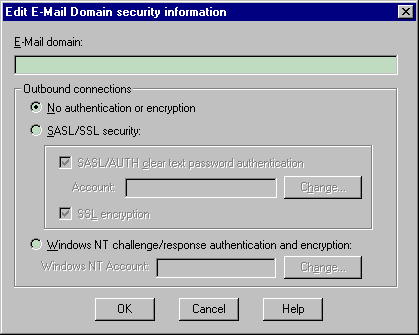
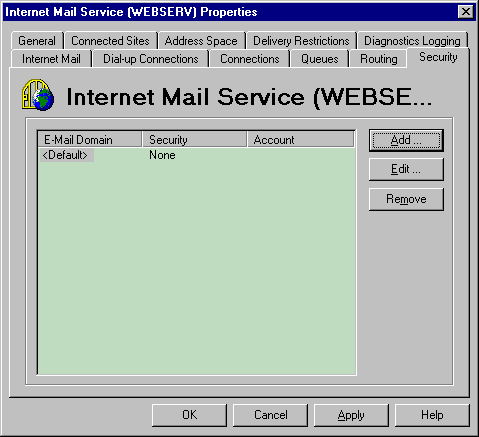
Поэтому рекомендуется по возможности использовать почтовый шлюз провайдера (с ним придется договориться) и всю почту принимать и отправлять только через него (естественно, шлюз провайдера должен поддерживать описанную выше схему). В этом случае не требуется аутентификация (вообще, не рекомендуется использовать аутентификацию там, где можно обойтись без нее). Но для этого MX запись в DNS-сервере зоны организации должна указывать на почтовый сервер провайдера, который, в свою очередь должен быть настроен на пересылку почты для ваших пользователей на ваш почтовый сервер.

Чтобы настроить использование почтового шлюза провайдера, необходимо отметить поле Forward all messages to host и указать имя или IP-адрес шлюза. Кроме того, администратор должен настроить прием соединений только от шлюза и хостов внутренней сети. Сотрудники организации, работающие за ее пределами, в качестве SMTP-сервера должны указывать шлюз провайдера.

Если невозможно использовать шлюз пройвайдера, рекомендуется использовать аутентификацию для всех хостов из внешней сети (Интернета).

Если и это невозможно, то администратор должен включить отслеживание всех попыток соединения и если он заметит признаки использования своего почтового сервера в качестве шлюза для рассылки спама, он должен сразу включить хост, с которого производилась рассылка, в список отвергаемых хостов (с помощью кнопки Specify by host) и принять меры для наказания рассыльщика (например, отправить письмо его провайдеру).

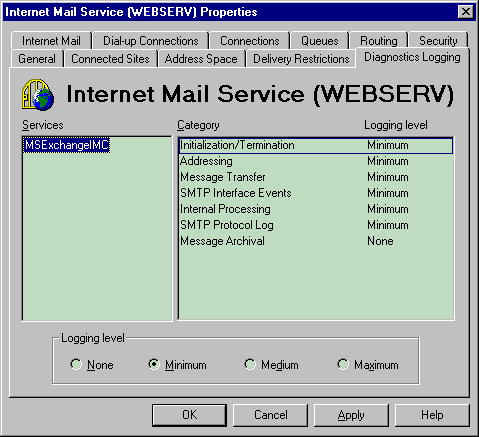
#### Security



Кнопка Add позволяет указать почтовые домены, при соединении с которыми сервер должен использовать SASL / SSL соединение (с аутентификацией или шифрованием), либо аутентификацию и шифрование Windows NT.

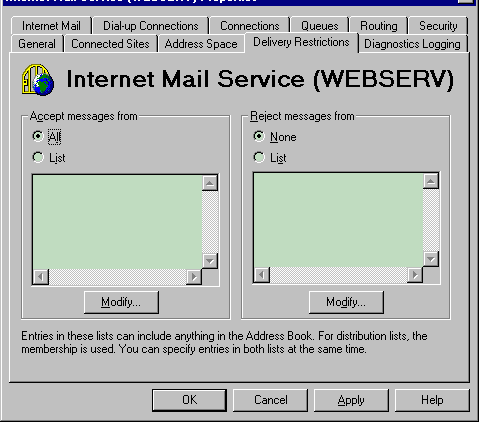
Для нашей организации рекомендуется оставить настройки без изменений.

#### Diagnostics Logging



В случае если используется схема без шлюза и аутентификации, рекомендуется поставить уровень протоколирования событий Message Transfer и SMTP protocol Log на Medium и каждый день проверять журнал событий Windows NT. В остальных случаях настройки оставляются на усмотрение администратора.

#### Delivery Restrictions



Здесь можно указать, от каких пользователей принимать сообщения (Accept messages from) и отвергать (Reject messages from). Рекомендуется оставить прием сообщений от всех пользователей, хотя в соответствии с политикой безопасности организации некоторые пользователи могут быть ограничены в правах.

# 

# Безопасность сервера IIS

Интернет-сервер (Internet Information Server, US) обеспечивает доступ по сети к файловым и вычислительным ресурсам компьютера с операционной системой Windows NT по протоколам HTTP, FTP, Gopher.

При подключении к Интернету информационные ресурсы становятся доступны огромному неконтролируемому сообществу, поэтому здесь администратор должен найти способ жестко ограничить спектр допустимых для пользователя действий.

## Введение в IIS

Рассмотрим вкратце назначение каждого из трех протоколов Интернет-сервера.

Проще всего передать информацию с одного компьютера на другой в виде файла данных, т.е. по протоколу передачи файлов (File Transfer Protocol, FTP). В этом протоколе используются обычные категории файловых систем: в каталогах, образующих древовидную структуру, находятся файлы данных.

Протокол Gopher предназначен для распределенных систем поиска и извлечения документов. Система Gopher использует концепцию каталога, содержащего отдельные документы. Каталоги Gopher можно расположить на разных компьютерах, при этом связав их в единую сетевую структуру. В последнее время протокол Gopher практически полностью вытеснен протоколом HTTP, поэтому в дальнейшем мы его рассматривать не будем.

Протокол передачи гипертекста (Hypertext Transfer Protocol, HTTP) служит для передачи информации вместе с признаком, указывающим тип данных. Изначальная цель его разработки — создание распределенных информационной систем, построенных по принципу гипертекста. Свидетельство успеха этого проекта — «Всемирная паутина» WWW (World Wide Web), основой которой как раз и является HTTP.

## 

## Анонимный и авторизованный доступ

### 

### Анонимный доступ

Проще всего при помощи IIS публиковать общедоступную информацию. При этом клиенты используют средства анонимного доступа, предусмотренные в каждом из протоколов IIS, и их подлинность не проверяется. В операционной системе Windows NT для работы таких вот «гостей из Интернета» выделяется специальная учетная запись пользователя. Программа установки IIS автоматически создает новую учетную запись с именем IUSR\_имя\_сервера, присваивает ей случайный пароль, и именно она используется в дальнейшем для обозначения гостей из Интернета. Администратор может указать и любую другую учетную запись. Потребность в смене учетной записи может возникнуть, например, если на нескольких серверах крупного Web-узла анонимный доступ к ресурсам должен осуществляться от одного и того же имени.

Таким образом, чтобы позволить обращаться к тому или иному ресурсу системы при анонимном доступе через IIS, администратор системы должен установить разрешения для данной учетной записи. Например, если папки, к которым возможен анонимный доступ, находятся на файловой системе NTFS, администратор может контролировать доступность отдельных файлов, регулируя права этой учетной записи, обозначенные в связанных с файлами списках разрешений.

### Авторизованный доступ

Организация авторизованного доступа к информации через IIS связана с целым рядом проблем. Прежде всего это вопрос производительности. Дело в том, что клиент HTTP сначала будет пытаться выполнить каждый запрос анонимно и только в том случае, если это не удастся, произведет повторный запрос с указанием имени и пароля пользователя. Дублирование запроса приводит к увеличению накладных расходов, а отсюда следует первое правило администратора: устанавливать авторизованный доступ только на ресурсы, действительно содержащие конфиденциальную информацию. Например, на файлы с текстом можно установить разрешения только для определенной группы пользователей, а доступ к файлам с графическими изображениями, которые вложены в текст и служат только для оформительских целей, разрешить и для учетной записи гостя из Интернета.

## Проверка подлинности в FTP

Стандарт на протокол FTP описан в RFC959.

Контроль доступа в FTP осуществляется простейшими средствами проверки подлинности пользователя. Для этого предусмотрены команды USER, PASS и АССТ — они передают по управляющему каналу имя и пароль пользователя, а также идентификатор учетной записи. Однако заметьте: эти параметры передаются в пакетах протокола IP в открытом виде. Поэтому злоумышленник, имеющий возможность перехватить пакеты сессии управляющего канала, легко узнает пароль пользователя.

Как и большинство других серверов FTP в Интернете, служба FTP из комплекта Windows NT, поддерживает возможность анонимного доступа к информации. Для этого пользователю нужно указать в команде USER специальное имя anonymous, а в качестве запрашиваемого пароля — ввести почтовый адрес, подлинность которого не проверяется и который применяется только для записи в журнал сервера FTP.

## Проверка подлинности в HTTP

Протокол НТТР/1.0 описан в RFC1945, формат MIME (Multipurpose Internet Mail Extensions) — в RFC1521. В январе 1997 года в виде RFC2068 опубликовано предложение по разработке нового стандарта HTTP/1.1, который должен существенно повысить производительность информационного обмена между клиентом и сервером.

Текущая версия протокола HTTP рассчитана в основном на анонимный доступ к серверу. Вместе с тем предусмотрена и возможность контроля доступа механизмами проверки подлинности типа вызов-ответ. Сервер HTTP из состава Windows NT может использовать две таких схемы: Basic и Windows NT Challenge-Response.

### Механизм Basic в HTTP

Клиент запрашивает сервер, указывая универсальный идентификатор ресурса URI. Сервер обнаруживает, что для доступа к ресурсу требуется идентификация пользователя, возвращает клиенту код ответа 401 (Unauthorized) и включает в сообщение строку заголовка, где указывается схема проверки подлинности, принимаемой сервером (Basic), и название области сети. в которую входит данный сервер. Все серверы в пределах одной области проверяют подлинность по одному списку пользователей.

Клиент может сделать следующий запрос к серверу, указав в первой строке запроса тот же идентификатор ресурса URL, но включив в сообщение строку заголовка, в которой передается имя и пароль пользователя, записанные через двоеточие и закодированные методом BASE64 (3 исходных байта кодируются 4 символами алфавита BASE64).

Таким образом, по схеме Basic пароль пользователя передается по сети в открытом виде.

### Механизм Windows NT Challenge-Response в HTTP

Вторая схема проверки подлинности, которая может использоваться для доступа клиента Internet Explorer к Интернет-серверу IIS, называется NTLM. Суть данной схемы состоит в том, что сервер в строке заголовка WWW-Authenticate передает клиенту «вызов» — последовательность 8 случайных байтов. Клиент применяет имеющийся у него хешированный пароль пользователя в качестве ключа шифрования и в заголовке Authorization возвращает серверу «ответ». В ответ включается имя пользователя, домен и зашифрованный паролем «вызов». Этой информации серверу достаточно, чтобы проверить подлинность пользователя и решить, передавать ли ему запрошенный ресурс.

Преимущество этого механизма в том, что во время проверки подлинности пароль по сети не передается. Однако применять его в глобальной сети Интернет вряд ли целесообразно. Во-первых, из клиентов HTTP в настоящее время его поддерживает только Microsoft Internet Explorer (начиная с версии 2). А во-вторых, он все же уязвим для изощренных атак, описанных ниже.

### Альтернативный подход: механизм Basic + протокол SSL

Протокол SSL (Secure Sockets Layer) предложен корпорацией Netscape для защиты от несанкционированного доступа передаваемых по Интернету данных путем их шифрования. С точки зрения архитектуры, SSL «встраивается» между модулями HTTP и TCP как на клиентском, так и на серверном компьютере. Поступающий от клиента HTTP-запрос сначала шифруется модулем SSL и в таком виде передается по каналу TCP. На сервере модуль SSL расшифровывает поступившие по каналу TCP данные и передает их HTTP-серверу. Ответ сервера в процессе передачи его клиенту подвергается аналогичным преобразованиям.

## Контроль допустимых операций

Рассмотренные выше средства контроля доступа основаны на идентификации и проверке подлинности пользователя, олицетворении его сервером и применении для защиты информации стандартных средств операционной системы. В дополнение к этому Интернет-сервер содержит средства ограничения допустимых операций протокола.

Администратор Интернет-сервера явно указывает папки файловой системы Windows NT, доступные по протоколам FTP, Gopher и HTTP, формируя отдельно для каждой из этих служб список виртуальных каталогов (virtual directories). Объявляя папку виртуальным каталогом IIS, администратор открывает доступ по сети ко всем файлам в этой и вложенных в нее папках. Для каждого виртуального каталога можно указать тип допустимых для него операций. Заметьте: рассматриваемые ограничения относятся ко всем обращающимся через виртуальный каталог пользователям.

Виртуальные каталоги могут быть вложены друг в друга, и эта вложенность не обязательно соответствует вложенности папок. Используя это средство, можно установить различные разрешения на подкаталоги виртуального каталога. Только помните: папка, имя которой длиннее 8 или содержит недопустимые для DOS символы, имеет в действительности два имени, и клиент в запросе может указать любое из них.

Операциями FTP являются считывание и запись информации. FТР-клиент выполняет операцию считывания по командам dir, get и mget. Операциям записи соответствуют команды клиента put, mput, delete, rename. По умолчанию все виртуальные каталоги FТР-сервера открыты только на чтение. Чтобы разрешить клиентам передавать файлы на сервер, администратору надо установить флажок Write в окне свойств соответствующего виртуального каталога.

Для службы HTTP в окне свойств каждого виртуального каталога администратор системы может разрешить или запретить выполнение по запросу клиентов операций Read и Execute.

Выполняемые приложения IIS (CGI, ISAPI), открывая большие возможности для создания нетривиальных информационных систем, одновременно представляют угрозу для системы безопасности сервера. Если приложение доступно через Интернет-сервер, его может запустить любой пользователь, располагающий стандартным клиентом HTTP. Поэтому администратору следует очень внимательно относиться к установке приложений IIS. Множество известных взломов защиты серверов HTTP связаны с эксплуатацией ошибок при администрировании Web-узла или ошибок установленных на нем приложений.

Microsoft рекомендует обычные и исполняемые файлы помещать в разные виртуальные каталоги, в свойствах виртуальных каталогов с обычными файлами разрешать только операцию Read, а с исполняемыми файлами — только Execute. Если в последнем случае разрешить обычное считывание, у клиентов появляется шанс получить копию исполняемого файла или сценария, а это — первый шаг к выявлению в этой программе ошибок и последующей их эксплуатации.

Тщательно контролируйте папки, объявленные виртуальными каталогами с разрешением исполнения приложений, и их подпапки. Установленные на них разрешения NTFS должны открывать их на запись лишь ограниченному кругу пользователей. Если приложениям требуется разрешение на запись в какие-либо файлы, лучше сделать так, чтобы эти файлы располагались в отдельной папке, недоступной через Интернет. Появление в виртуальных каталогах с приложениями файлов с расширениями .exe, .com, .dll — очень тревожный признак. В реестре операционной системы периодически проверяйте список интерпретаторов сценариев, а также значение параметра HKEY\_LOCAL\_MACHINE\SYSTEM\Current-ControlSet\Services\W3SVC\Parameters\Filter DLLs, в котором перечисляются дополнительные библиотеки, подключаемые к Интернет-серверу.

Среди операций сервера HTTP есть еще одна, не упоминавшаяся ранее — Browse. Что сделает Интернет-сервер, если в запросе указано имя папки, а не файла? По умолчанию — будет искать в этой папке файл default.htm и возвратит клиенту его содержимое. Но если такого файла нет, он может составить индекс, т.е. перечислить имеющиеся в ней файлы и подпапки. Для информационных систем, созданных по типу WWW, это излишняя операция, поскольку доступ к отдельным файлам осуществляется по гипертекстным связям. Поэтому по умолчанию этот параметр всегда отключен. Однако иногда разработчики Web-узлов, публикуя большое количество файлов, не утруждают себя созданием и поддержанием в актуальном состоянии гипертекстного индекса. В этом случае удобно воспользоваться средством автоматического составления индекса папки. Во второй и третьей версиях IIS оно включается установкой флажка Browsing в окне свойств службы WWW Интернет-сервера на вкладке Directories.

## Возможные атаки

Сервер IIS для проверки подлинности использует базу учетных записей Windows NT. С одной стороны, это позволяет легко регулировать доступ к ресурсам системы. С другой — при определенных условиях злоумышленник может узнать пароль, указанный пользователем в процессе проверки сервером IIS его подлинности. В таком случае этот пароль можно применить не только для доступа через IIS, но и для любых других операций в сети.

### Перехват пароля

При проверке подлинности по протоколам FTP и HTTP (Basic) пароль пользователя передается по сети открытым текстом. Любой злоумышленник, способный перехватить пакеты, идущие от клиента к серверу, легко узнает этот пароль. Поэтому применять эти механизмы не рекомендуется.

### Подбор пароля

Механизм проверки подлинности NTLM несколько более защищен. Однако. перехватив пару «вызов-ответ», злоумышленник может применить программу простого перебора и восстановить пароль пользователя. Возможность этой атаки усугубляется тем, что, во-первых, Internet Explorer для Windows 95 и Windows NT 4 передает на сервер имя и пароль пользователя, даже не оповещая последнего об этом. А во-вторых, по сети передается результат шифрования, основанный на пароле LAN Manager, который защищен сравнительно слабо.

### Использование хешированного пароля

Чтобы пройти проверку подлинности на IIS, клиенту не нужно знать исходный пароль пользователя, достаточно иметь 16-байтовый хешированный пароль. Получить его можно с помощью программы PWDump. Тем самым еще раз подчеркнем: база учетных записей компьютеров нуждается в защите.

### Атака Man-in-the-Middle

Атака на механизм «вызов-ответ», называемая Man-in-the-Middle, может быть с минимальными изменениями проведена по протоколу HTTP.

1. Пользователь Internet Explorer пытается получить доступ к WEB-серверу злоумышленника. Тот идентифицирует «жертву» и инициирует проверку подлинности по механизму NTLM.

2. Злоумышленник издает запрос на атакуемый сервер в домене жертвы, чтобы открыть сессию SMB.

3. Сервер генерирует злоумышленнику ответ, содержащий случайный «вызов».

4. Система злоумышленника транслирует этот же «вызов» по протоколу HTTP.

5. Internet Explorer, применив пароль пользователя, формирует «ответ» и передает его на проверку злоумышленнику.

6. Злоумышленник транслирует «ответ» пользователя атакуемому серверу и, естественно, получает к нему доступ.

Самое неприятное в этой атаке то, что пользователь может даже не подозревать, что сведения о нем переданы на сервер в Интернете.

## Рекомендации по защите сервера IIS

### Типовые потребности организации

Рассматриваемая нами типовая организация обычно нуждается в IIS для предоставления пользователям Интернета доступа к Web-серверу организации по протоколам HTTP и FTP.

Механизм аутентификации не нужен, так как нет потребности ограничивать доступ к ресурсам Web-сервера ни из Интернета, ни из внутренней сети организации.

Для обеспечения таких потребностей достаточно IIS 3, входящего в состав NT Service Pack 3 и выше. Если требуются дополнительные возможности (например, поддержка IIS), лучше установить IIS 4, который доступен в составе бесплатно распространяемого Windows NT Option Pack.

### Инсталляция сервера IIS

Если IIS не был установлен в процессе инсталляции Windows NT, то его можно инсталлировать, запустив файл inetins.exe из директории %SystemRoot%\system32.

Так как Web-сервер нашей типовой организации размещен в локальной сети, для его работы через прокси-сервер необходимы некоторые специальные настройки:

1. На компьютере, выполняющем роль Web-сервера, должен быть инсталлирован WinSock Proxy client.

2. Необходимо создать текстовый файл wspcfg.ini и поместить его в директорию с файлом inetinfo.exe (%SystemRoot%\system32\inetsrv). Содержимое файла wspcfg.ini:

[inetinfo]

ServerBindTcpPorts=21,20,80

LocalBindTcpPorts=20

KillOldSession=1

Persistent=1

Forcecredentials=1

3. Если используется разграничение доступа в Интернет, необходимо создать специальную учетную запись, от имени которой будет происходить авторизация службы Web-сервера в MS Proxy Server’e (например, “InetInfo”). Далее, необходимо с помощью утилиты CredTool, входящей в состав WinSock Proxy Client, указать файлу inteinfo.exe действовать от имени этой учетной записи. Для нашего примера это будет команда credtool –w –n inetinfo –c InetInfo domain password

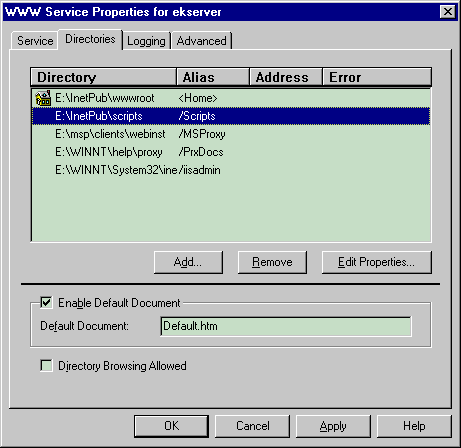
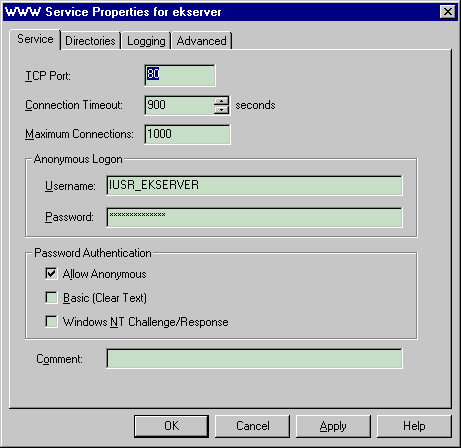
4. В свойствах WinSock необходимо создать два протокола:

|  |  |  |
| --- | --- | --- |
| Параметр | 1 | 2 |
| Protocol Name | FTP Server | HTTP Server |
| Initial Connection | 21 TCP Inbound | 80 TCP Inbound |
| Port Range | 1025-500 | - |
| Type | TCP | - |
| Direction | Inbound |  |

5. Разрешить работать через эти протоколы учетной записи, от имени которой действует служба IIS («InetInfo»).

6. Инсталлировать заплатку с сервера Microsoft (http://support.microsoft.com/support/kb/articles/Q236/0/01.ASP).

### Настройка службы WWW



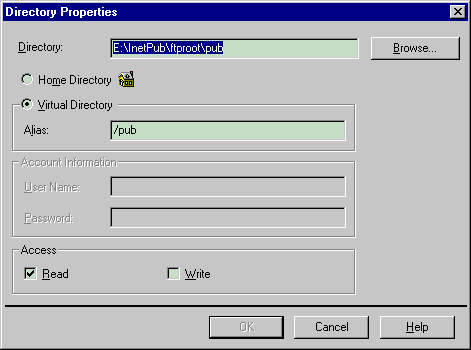
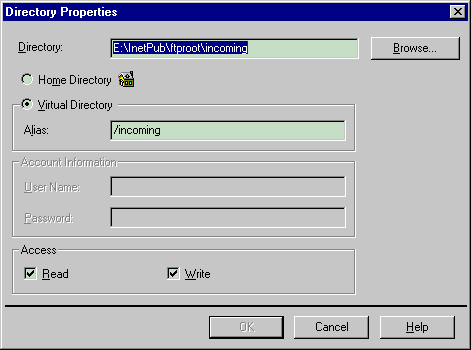
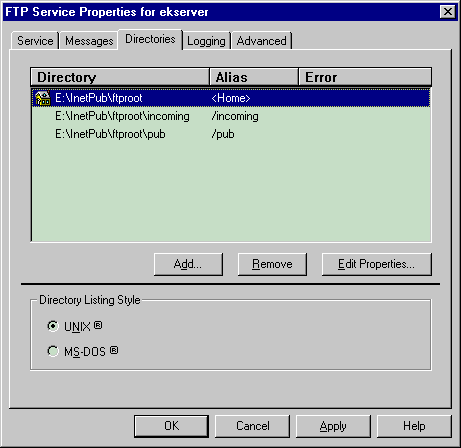
Основные настройки приведены на рисунках выше.

Следует обратить внимание, что для папки /Scripts следует установить только разрешение Execute, для остальных – Read.

### Настройка службы FTP

Как это принято в Интернет, рекомендуется в FTP-директории создать папки pub и incoming. Из папки pub посетитель может только читать информацию, а в папку incoming – только записывать. Для этого необходима довольно сложная комбинация разрешений NTFS и IIS.

Настройки IIS приведены на рисунках ниже. В них предполагается, что компьютер имеет имя EKSERVER и созданный по умолчанию пользователь, которым олицетворяется IIS-анонимный пользователь, называется IUSR\_EKSERVER.



Разрешения NTFS для пользователя IUSR\_EKSERVER приведены в списке:

1. Для папки ftproot – Read (RX)(RX);
2. Для папки incoming – Special Access (RW)(W);

3. Для папки pub – Read (RX)(RX).

### Дополнительные меры защиты

Не рекомендуется Web-дизайнерам и Web-программистам давать доступ к WWW-директориям по протоколу FTP. Вместо этого лучше сделать ее доступной по внутренней сети и работать только оттуда.

Рекомендуется отслеживать и хранить лог-файлы IIS в течение длительного времени. Быть может, эти файлы годичной давности помогут доказать вам, что атака на Bank of New York с вашего сервера была произведена не вами, а кем-то, кто ранее сумел взломать его.

При наличии невысокоскоростного канала в Интернет рекомендуется ограничить максимальную скорость доступа к Web-серверу, чтобы какая-то часть канала всегда была доступна вашим пользователям. По этой же причине (а также в зависимости от мощности Web-сервера) лучше ограничить максимальное число FTP и HTTP-соединений.

Разделы реестра HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots и HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MSFTPSVC\Parameters\Virtual Roots рекомендуется открыть для полного доступа только ОС и администраторам.

Отслеживать появление в каталогах IIS неизвестных файлов, особенно с расширениями com, exe, dll в папках с разрешением Execute.

Следить, чтобы удаленный пользователь не мог по протоколу FTP, закачав в папку incoming большое количество информации, переполнить жесткий диск Web-сервера.