Серверы безопасности и их функции. Брандмауэры. Прокси-серверы

1. Серверы безопасности и их функции

Обеспечение безопасности web-серверов

В самом общем виде web можно разделить на два основных компонента: web-серверы — они являются приложениями, которые формируют информацию, доступную по протоколу HTTP, и web-браузеры (клиенты) — они используются для доступа и показа информации, хранящейся на web-серверах. В основном будем рассматривать проблемы безопасности, касающиеся web-серверов.

К сожалению, web-серверы часто являются целями атак. Вследствие этого важно гарантировать безопасность web-серверов, а также сетевой инфраструктуры, которая их поддерживает. Угрозы безопасности, специфичные для web-серверов в общем случае можно разделить на следующие категории:

- **Враждебно настроенные пользователи интернета могут использовать ошибки ПО в web-серверах лежащей в основе ОС или в программах, создающих динамические web-страницы, для получения неавторизованного доступа к web-серверу.**

1. **Результатом этого может быть получение доступа к файлам или каталогам, которые не предназначены для открытого доступа, либо выполнение привилегированных команд и/или установка ПО на web-сервер.**
2. **Информация на web-сервере может быть преднамеренно изменена с враждебными целями. Наиболее общим примером такой угрозы является подмена содержимого web-сайта.**

- **Denial of service (DoS) атаки могут быть направлены на web-сервер что приведет к отказу в доступе законным пользователям.**

- **Чувствительная информация, передаваемая в открытом виде между web-сервером и браузером, может быть перехвачена.**
- **Пользователи могут получить неавторизованный доступ к ресурсам, расположенным где-то еще в локальной сети организации, используя успешную атаку на web-сервер.**
- **Возможно осуществление атаки на другие сети и серверы, причем будет использован скомпрометированный web-сервер, скрыта настоящая идентификация и, иногда, ответственность за последствия возложена на администратора web-сервера, с которого выполняется атака.**

- **Сервер может быть использован в качестве незаконной точки распространения ПО, инструментальных средств атаки, при этом на администратора сервера может быть возложена ответственность за последствия атаки.**

Рассмотрим проблемы, связанные с безопасностью при инсталлировании, конфигурировании и сопровождении web-серверов.

Перечислим кратко основные вопросы:

- **Безопасное инсталлирование и конфигурирование лежащей в основе ОС.**
- **Безопасное инсталлирование и конфигурирование ПО web-сервера.**
- **Развертывание соответствующих сетевых механизмов защиты:**
  - **Firewall’ы;**
  - **Intrusion detection systems (IDS);**
  - **DNS.**

- **Поддержка безопасной конфигурации, со своевременным применением соответствующих patches и upgrades, тестированием безопасности, просмотром логов и выполнение backup’ов как данных, так и ОС.**
- **Обеспечение защиты информации, исходя из ее семантики.**

Здесь нужно придерживаться следующих принципов.

Следует реализовать соответствующую практику управления безопасностью и контроль за функционированием системы.

Для гарантирования безопасности web-сервера и поддержки сетевой инфраструктуры должны быть рассмотрены и реализованы следующие основные моменты:

- **Политика безопасности информационной системы организации.**
- **Принципы управления и контроля конфигурации и ее изменений.**
- **Анализ риска и определенные подходы к управлению риском.**
- **Стандартные конфигурации ПО, которые удовлетворяют политике безопасности информационной системы.**

- **Необходимый объем знаний и тренинги, обеспечивающие требуемый объем знаний.**
- **Способы восстановления после внезапных сбоев.**
- **Соответствующая сертификация и аккредитация.**

Следует гарантировать, что ОС, на которой выполняется web-сервер, развернута, сконфигурирована и управляется в соответствии с требованиями безопасности.

Первым шагом в обеспечении безопасности web-сервера является безопасность лежащей в основе ОС. Большинство доступных web-серверов выполняются на ОС общего назначения. Многих проблем безопасности можно избежать, если ОС, лежащая в основе web-сервера, сконфигурирована соответствующим образом. Конфигурации по умолчанию для аппаратуры и ПО обычно устанавливаются производителями, при этом, как правило, делается упор на использование возможностей, функциональностей исходного ПО, а также на простоту использования возможностей, связанных с безопасностью.

Также следует понимать, что производители не знают требований безопасности каждой организации, поэтому web-администратор должен сконфигурировать новые серверы в соответствии с требованиями безопасности и переконфигурировать их каждый раз при изменении этих требований. Обеспечение безопасности ОС как минимум должна включать следующие шаги:

- **выполнение patch'ей и upgrade'ов ОС;**
- **удаление или запрещение ненужных сервисов и приложений;**
- **конфигурирование управления ресурсами;**
- **тестирование безопасности ОС.**

Обеспечение безопасности web-сервера как минимум должно включать следующие шаги:

- **выполнение patch'ей и upgrade'ов ПО web-сервера – удаление или запрещение ненужных сервисов, приложений и примеров содержимого;**
- **конфигурирование аутентификации пользователей web-сервера ;**
- **конфигурирование управления ресурсами web-сервера ;**
- **тестирование безопасности приложения web-сервера и конкретного содержимого web-сервера.**

Следует предпринять шаги для гарантирования того, что на web-сайте публикуется только корректное содержимое.

Необходимо защищать содержимое web посредством выполнения соответствующего управления ресурсами web-сервера. Некоторые примеры управления ресурсами включают:

- **инсталлирование только необходимых сервисов;**
- **инсталлирование web-содержимого на выделенном жестком диске или в выделенном разделе;**
- **возможность выполнять запись (uploads) только в директории, которые не являются читаемыми из web-сервера, а доступны по некоторому другому протоколу (например, ftp);**

- **определение единственной директории для всех скриптов или программ, которые выполняются для создания web-содержимого и являются внешними по отношению к web-серверу ;**
- **запрещение использования жестких или символических ссылок в файловой системе ОС, на которой выполняется web-сервер ;**
- **создание матрицы доступа к web-содержимому, которая определяет, какие папки и файлы внутри директории web-сервера имеют ограничения по доступу;**
- **запрет просмотра директории в файловой системе;**
- **использование аутентификации пользователей с помощью цифровых подписей и других криптографических механизмов.**

Поддержание безопасного функционирования web-сервера требует постоянных усилий и наличия достаточного количества ресурсов. Поддержание безопасности web-сервера обычно включает следующие шаги:

- **своевременное применение patch'ей и upgrade'ов;**
- **конфигурирование, защита и анализ лог файлов;**
- **частое выполнение back up'а критической информации;**
- **поддержка защищенных копий web-содержимого;**
- **определение процедур восстановления при компрометации и следование им при обнаружении проникновения;**
- **периодическое тестирование безопасности.**

Причины уязвимости web-сервера

Основные проблемы, связанные с безопасностью функционирования публично доступного web-сайта, возникают по следующим причинам:

- **Неправильная конфигурация или другое некорректное действие над web-сервером, которое может привести к раскрытию или изменению информации.**

- **Уязвимости ПО web-сервера, которые могут допускать, например, чтобы атакующий компрометировал безопасность сервера или других хостов в сети.**
- **Неадекватные механизмы защиты web-сервера, предусмотренные в его окружении.**
- **ПО на стороне сервера (скрипты, JSP, ASP и т.п.), которое содержит ошибки, позволяющие атакующим компрометировать безопасность web-сервера.**

2. Брандмауэры и их функции

Мало кто сегодня не слышал об угрозах, существующих в виртуальном пространстве. Пока еще остается непреложным тот факт, что компьютер, подсоединенный к сети Интернет, может подвергнуться реальным атакам. К сожалению, нередко встречаются неадекватные или незаконопослушные люди (часто в одном лице), патологически не способные существовать без того, чтобы не портить жизнь другим. Тех из них, которые разбираются в компьютерах и знают, как получить удаленный доступ к файлам, называют хакерами. Чтобы защититься от них, нам прежде всего нужен хороший брандмауэр.

Перечислим основные опасности, существующие в Сети:

- **Приложения-нарушители могут «поселиться» и запускаться на вашем компьютере незаметно для вас (например, ActiveX или Java-апплеты, внедренные в web-страницу, которую вы просматриваете). Эти приложения могут выполнить любую операцию на вашем компьютере, в том числе переслать файлы с вашей частной информацией другим компьютерам или вообще удалить данные из вашей системы.**
- **При неправильной настройке системы другие компьютеры могут получить доступ к вашим файлам напрямую, без загрузки специального**

- **Некоторые виды информации (cookies или referrers) могут быть размещены на вашем компьютере таким образом, что заинтересованные лица смогут следить за вашими действиями в Сети и будут знать о ваших интересах.**
- **Троянские кони также представляют угрозу компьютеру. «Троянцы» — это программы, используемые хакерами, которые раскрывают вашу частную информацию (пароли, реквизиты, номера кредитных карт). Одно из главных различий между «троянцем» и вирусом — это то, что вирус действует на компьютере автономно, а троянский конь напрямую управляется взломщиком из Сети.**

- **Интернет-черви обычно проникают в компьютер вместе с почтой, в виде вложений. Некоторые почтовые программы открывают вложения самостоятельно. Неопытные пользователи, не осознавая угрозы, открывают вложения сами. Если открыть такое послание хотя бы один раз, то выполняющийся «червь» начнет стремительно поражать систему.**
- **Масса ненужного трафика в виде баннеров и сообщений снижает пропускную способность компьютера. Хотя эти объекты не могут нанести прямой вред данным, они значительно замедляют скорость соединения, особенно осуществленного посредством телефонной линии.**

- **Шпионские программы во многом похожи на «троянцев». Они собирают сведения о ваших интересах (посещаемые сайты, установленное программное обеспечение и т.д.) без вашего ведома и согласия.**

В настоящее время большинство локальных вычислительных сетей (ЛВС) подключены к сети Интернет. Однако отсутствие эффективных средств защиты информации в существующих сетевых протоколах приводит к различным нарушениям целостности передаваемых данных.

Общее описание брандмауэров

Брандмауэр (firewall, межсетевой экран) — это система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения информации из одной части в другую. Брандмауэры представляют собой целый класс систем, порой сопоставимых по сложности с операционной системой. Классифицировать их можно по исполнению: программные, аппаратные и смешанного типа (аппаратно-программного); по компонентной модели: локальные (работающие на одном хосте) и распределенные (distributed firewall). Однако самой «полезной» является классификация с точки зрения уровня, на котором функционируют брандмауэры: пакетный уровень, прикладной, уровень соединения.

Разбивка на уровни является условной, что подразумевает возможность работы отдельно взятого брандмауэра более чем на одном уровне одновременно. Можно сказать, что практически все современные брандмауэры функционируют сразу на нескольких уровнях, стремясь расширить функциональность и максимально использовать преимущества работы по той или иной схеме. Такая технология получила название Stateful Inspection, а брандмауэры, работающие по смешанной схеме, называются Stateful Inspection Firewall.

Пакетный уровень

Работа на пакетном уровне заключается в фильтрации пакетов. Решение о том, пропускать данный пакет или нет, принимается на основе следующей информации: IP-адреса, номера портов отправителя и получателя, флаги. По сути, задача администратора сводится к составлению простенькой таблицы, на основании которой осуществляется фильтрация.

Преимущества пакетного уровня:

- низкая стоимость;

- высокая производительность.

Недостатки:

- сложность конфигурирования и поддержки;

- отсутствие дополнительных возможностей;

- рухнувшая сеть остается открытой (не защищенной);

- не защищены от фальсификации IP- и DNS-адреса.

Прикладной уровень

Фильтрация на уровне пакетов, конечно, очень проста, но нередко ее бывает явно недостаточно. Информации сетевого и транспортного уровня модели OSI иногда не хватает для эффективной работы, что обусловливает существование систем, работающих на самом верхнем уровне — прикладном. Фактически брандмауэры данного уровня предоставляют собой несколько отдельных подсистем (так называемых application gateways — серверов прикладного уровня), по числу обслуживаемых сервисов. Между пользовательским процессом и нужным сервисом возникает посредник, пропускающий через себя весь трафик и принимающий в рамках установленной политики безопасности решение о его легитимности.

Преимущества прикладного уровня:

- маскировка защищаемой сети;

- широкие возможности (усиленная аутентификация, детальное протоколирование);

- рухнувшая сеть остается заблокированной (защищенной).

Недостатки:

- высокая стоимость;

- низкая производительность.

Уровень соединения

Шлюз на уровне соединения представляет собой систему, транслирующую соединения вовне. При установлении доступа пользовательский процесс соединяется с брандмауэром, который, в свою очередь, самостоятельно устанавливает соединение с внешним узлом. Во время работы брандмауэр просто копирует входящую/исходящую информацию. По большому счету данный шлюз надо рассматривать не как самостоятельный и самодостаточный механизм, а лишь как специфическое решение некоторых задач (например, для работы с нестандартными протоколами, если необходимо создать систему сбора статистики для какого-то необычного сервиса, предоставить доступ только к определенным внешним адресам, осуществить базовый мониторинг и т. д.).

Функции брандмауэров

Идеальный персональный брандмауэр должен выполнять шесть функций:

- **Блокировка внешних атак В идеале брандмауэр должен блокировать все известные типы атак, включая сканирование портов, IP-спуффинг, DoS и DDoS, подбор паролей и пр.**
- **Блокировка утечки информации Даже если вредоносный код проник в компьютер (не обязательно через сеть, а, например, в виде вируса на купленном пиратском CD), брандмауэр должен предотвратить утечку информации, заблокировав вирусу выход в сеть.**

- **Контроль приложений Неизбежное наличие открытых дверей (то есть открытых портов) является одним из самых скользких мест в блокировке утечки информации, а один из самых надежных способов воспрепятствовать проникновению вирусов через эти двери — контроль приложений, запрашивающих разрешение на доступ. Кроме банальной проверки по имени файла, весьма желательна проверка аутентичности приложения.**

- **Поддержка зональной защиты Работа в локальной сети часто подразумевает практически полное доверие к локальному контенту. Это открывает уникальные возможности по использованию новейших (и, как правило, потенциально опасных) технологий. В то же время уровень доверия к Интернет-контенту значительно ниже, а значит, необходим дифференцируемый подход к анализу опасности того или иного содержания.**

- **Протоколирование и предупреждение Брандмауэр должен собирать строго необходимый объем информации. Избыток (равно как и недостаток) сведений недопустим. Возможность настройки файлов регистрации и указания причин для привлечения внимания пользователя приветствуются.**
- **Максимально прозрачная работа Эффективность и применяемость системы часто обратно пропорциональны сложности ее настройки, администрирования и сопровождения. Несмотря на традиционный скепсис в отношении «мастеров» (wizards) по настройке и прочих буржуйских штучек, даже опытные администраторы не пренебрегают ими просто в целях экономии времени.**

Недостатки брандмауэров

Нельзя забывать и об обратной стороне медали, о недостатках, причем не отдельных решений, а всей технологии в целом.

Разрозненность систем защиты

Это одна из самых важных проблем, решить которую пытаются немало поставщиков, но пока без особого успеха. Во многих брандмауэрах отсутствует защита от саботажа со стороны авторизованных пользователей. Этот вопрос можно рассматривать с этической, социальной или любой другой точки зрения, но сути дела это не меняет — брандмауэры не способны запретить авторизованному пользователю украсть (передать вовне, уничтожить, модифицировать) важную информацию.

Отсутствие защиты для нестандартных или новых сетевых сервисов

Решением здесь в какой-то мере могут служить шлюзы на уровне соединения или пакетные фильтры, но, как уже говорилось, им недостает гибкости. Конечно, существуют определенные возможности по туннелированию нестандартного трафика, например в HTTP, но этот вариант нельзя назвать удобным сразу по нескольким причинам. Есть множество унаследованных систем, код которых переписать невозможно. Однако оставлять их беззащитными тоже нельзя.

Снижение производительности

К счастью, подобные вопросы возникают все реже и реже, особенно у частных пользователей, стремящихся защитить свой ПК или небольшую локальную сеть. В то же время крупные локальные сети по-прежнему генерируют столь емкий трафик, что обычными программными (дешевыми или бесплатными) решениями сеть не прикроешь. Аппаратные решения демонстрируют отличную производительность и масштабируемость, но вот цена (порой исчисляемая десятками тысяч долларов) переводит вопросы их применения в совершенно иную плоскость, так что порой максимум возможного — это выделение специального сервера, «заточенного» исключительно под обслуживание брандмауэра.

Общие принципы настройки Firewall

Конфигурация firewall — предмет достаточно сложный, и обычно все сетевые экраны (firewall) имеют индивидуальную конфигурацию, отражающую специфику работы конкретной информационной системы. Однако здесь следует придерживаться некоторых общих принципов:

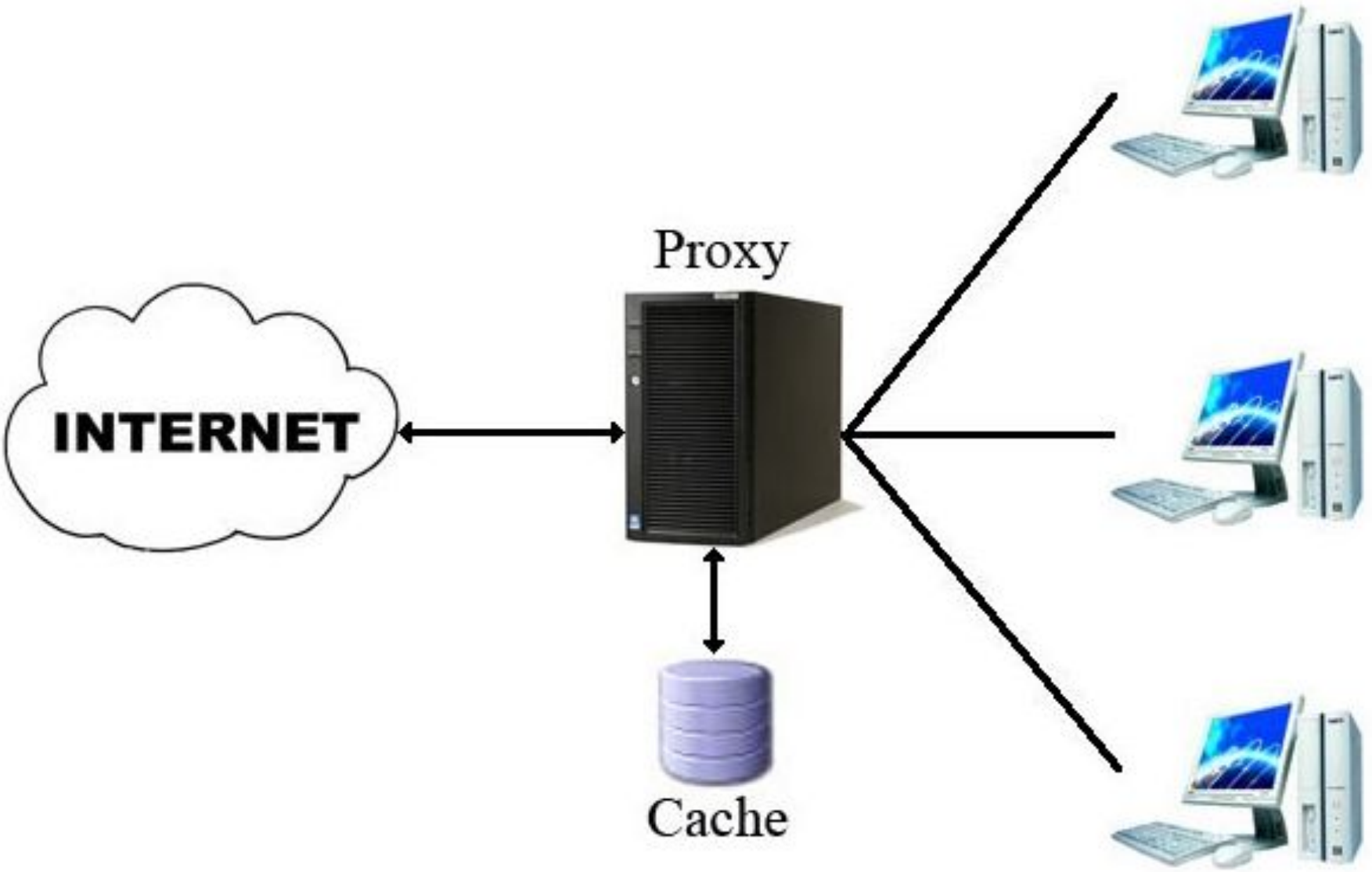
Следует пропускать сквозь себя только те сервисы, которые необходимы для обеспечения требуемой функциональности информационной системы.

Все, что явным образом не разрешено, должно быть запрещено. Это означает, что все службы, не упомянутые при конфигурации firewall, должны быть запрещены.

При конфигурации сетевых экранов (firewall) следует вести подробную документацию.

3. Прокси-серверы и их функции

Прокси-сервер является сервером, который расположен между клиентским компьютером и фактическим сервером в интернете. Прокси-сервер исполняет роль перехвата каждого запроса к запрашиваемому серверу и контроля возможности доступа к желаемому адресу в интернете. Если это оказывается невозможным, то прокси направляет запрос на другой сервер.


Proxy
INTERNET
Cache

Основные функции прокси-сервера

При использовании на предприятии прокси-сервер, кроме доступа в интернет, т.е. основной своей роли, также несет функцию обеспечения контроля и безопасности. Являясь сервером шлюза, прокси-сервер играет роль разделения сети предприятия от других сетей.

Интернет прокси-сервер также связан с функцией брандмауэра, который используется для защиты сети предприятия от любых вторжений извне.

Принцип работы прокси-сервера

Интернет прокси-сервер, получая запросы от веб-страниц или любых других интернет пользователей, проверяет их на возможность выполнения с учетом заданной фильтрации. При выполнении всех условий прокси-сервер проверяет свой кэш для запрашиваемых страниц (это в случае, если прокси-сервер является кэш-сервером). Если веб-страницы, куда отправлен запрос найдены, то они возвращаются пользователю. В этом случае нет необходимости в прокси-сервере, как в инструменте для переадресации запроса. В случае если страница не может быть найдена в кэше, то прокси-сервер выступает в качестве клиента, используя собственный IP-адрес, запрашивая веб-страницу с других серверов, которые находятся в интернете.

Классификация proxy серверов.

Существует несколько типов proxy серверов. Каждый тип proxy предназначен для решения своего круга задач, однако у них есть много общего, их возможности во многом совпадают.

HTTP proxy

Это наиболее распространенный тип proxy серверов и говоря просто "proxy", имеют в виду именно его. Раньше с помощью этого типа proxy можно было только просматривать web страницы и картинки, скачивать файлы. Теперь же новые версии программ (ICQ и т.п.) умеют работать через HTTP proxy. С этим типом proxy умеют работать и браузеры любых версий.

Socks proxy

Эти proxy сервера умеют работать практически с любым типом информации в Internet (протокол TCP/IP), однако для их использования в программах должно быть явно указана возможность работы с socks proxy. Для использования socks proxy в браузере нужны дополнительные программы (браузеры не умеют сами работать через socks proxy). Однако любые версии ICQ (и многих других популярных программ) отлично могут работать через socks proxy. При работе с socks proxy необходимо указывать его версию: socks 4 или socks 5.

CGI proxy (анонимайзеры)

С этим типом proxy серверов можно работать только через браузер. В других программах их использование затруднено (да и не нужно - есть HTTP proxy). Однако поскольку этот тип proxy изначально рассчитан на работу через браузер, использовать их исключительно просто. Вы легко сможете не только задействовать анонимайзер в своей работе, но и без проблем построить цепочку из CGI proxy.

FTP proxy

Этот тип proxy серверов отдельно от корпоративных сетей встречается довольно редко. Обычно его использование связано с тем, что в организации имеется Firewall (система защиты компьютеров от вторжения извне), препятствующий прямому доступу в Internet. Использование proxy этого типа предусмотрено во многих популярных файловых менеджерах (FAR, Windows Commander), download менеджерах (GetRight, ReGet, ...) и в браузерах.

Этот тип proxy является узко специализированным и предназначен для работы только с FTP серверами.

HTTPS-прокси

HTTPS-прокси– фактически частьHTTP-прокси.S в названии означает “secure”, т.е. безопасный. Не смотря на то, что программно это часть HTTPпрокси, обычно HTTPS выделяют в отдельную категорию (и есть отдельное поле для него в настройке браузеров). Обычно этот протокол – безопасный HTTP – применяют, когда требуется передача секретной информации, например, номеров кредитных карт. При использовании обычного HTTPпрокси всю передаваемую информацию можно перехватить средствами самого прокси (т.е. это под силу адми нистратору ЛС) или на более низком уровне, например, tcpdump.

Mapping-прокси

Mapping-прокси– способ заставить работать через прокси те программы, которые умеют работать с интернетом только напрямую. При настройке такого прокси администратор создает как бы «копию» целевого сервера, но доступную через один из портовпрокси-серверадля всех клиентов локальной сети – устанавливает локальное «отображение» заданного сервера. Например, пользователи локальной сети хотят работать с почтовым сервером mail.ru не через браузер, а с использованием почтовой программы Outlook Express или TheBat. Эти программы не умеют работать через прокси (кроме случая, когда Outlook получает почту по HTTP с hotmail.com – тогда он, как и браузер, пользуетсяHTTP-прокси).

Простейший способ работать с mail.ru по POP3 через прокси – установить локальное отображение сервера pop.mail.ru. И в Outlook'ах вместо pop.mail.ru написать имяпрокси-сервераи порт отображения. Outlook будет соединяться спрокси-сервером("думая", что это почтовый сервер), а прокси при этом будет соединяться с pop.mail.ru и прозрачно передавать всю информацию между Outlook и pop.mail.ru, таким образом «превращаясь» на время соединения вPOP3-сервер. Неудобствомapping-проксив том, что для каждого необходимого внешнего сервера нужно вручную устанавливать отдельный порт на прокси. Но зато не требуется модификация ни серверов, ни клиентов.

Особенно это помогает в случае необходимости «проксирования» многочисленных «доморощенных» протоколов, реализованных в играх или финансовых программах.Почему-тоони часто игнорируют существование прокси и стандартных протоколов. Такие программы можно «обмануть» и направить через прокси практически всегда, если они не делают другой глупости – передачи клиентскогоIP-адресавнутри протокола и пытаются с ним соединяться напрямую еще раз (что невозможно, т.к. локальные адреса.