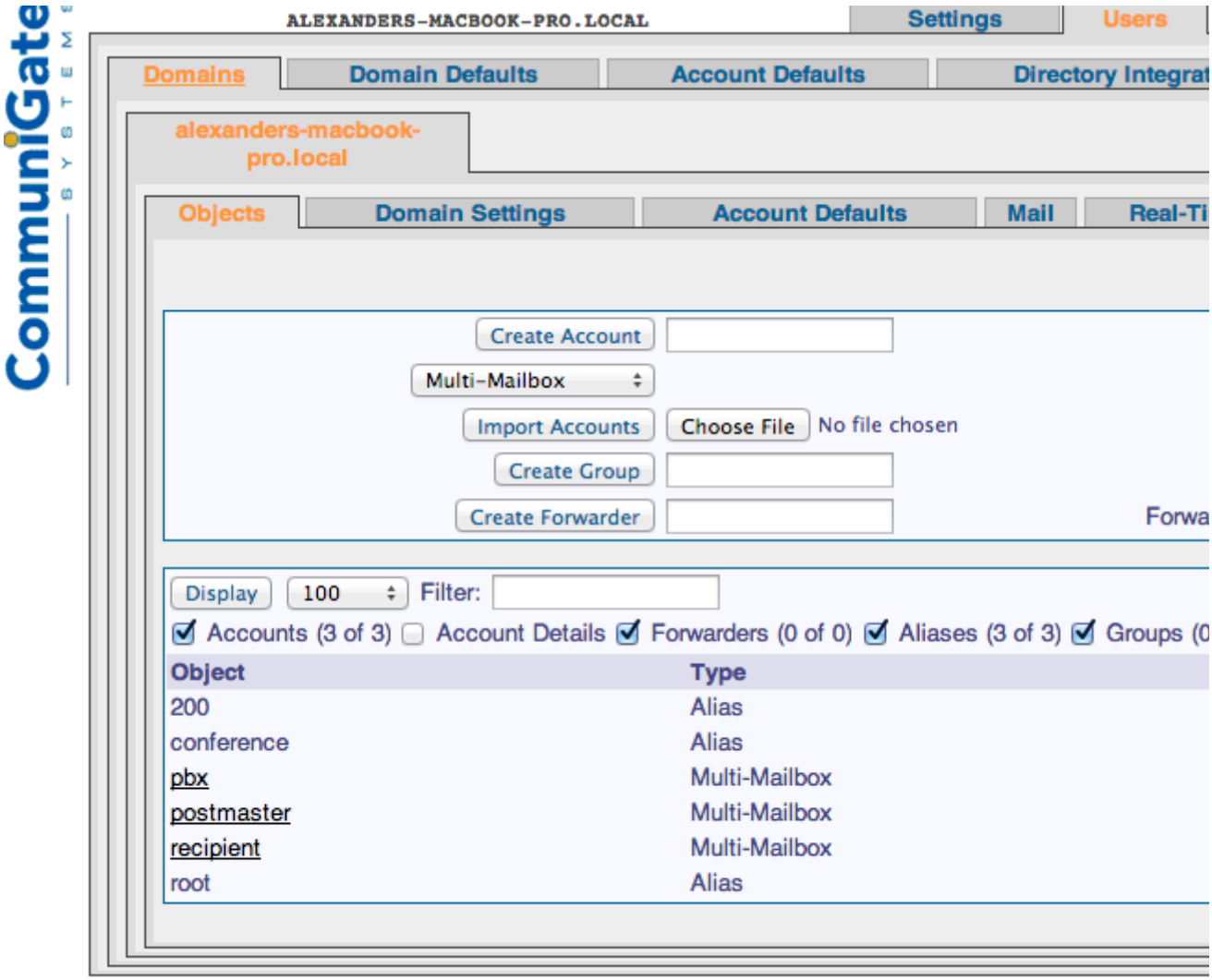
Теоретический минимум для администратора почты. Настройка почты на сервере Communigate Pro

В этой статье приведена базовая информация, которую нужно знать для того, чтобы начать администрировать почтовый сервер, некоторая часть текста (~30%) касается стандартных протоколов, либо широко применяемых практик и поэтому актуальна не только для Communigate Pro.

Админка

Создание учетных записей

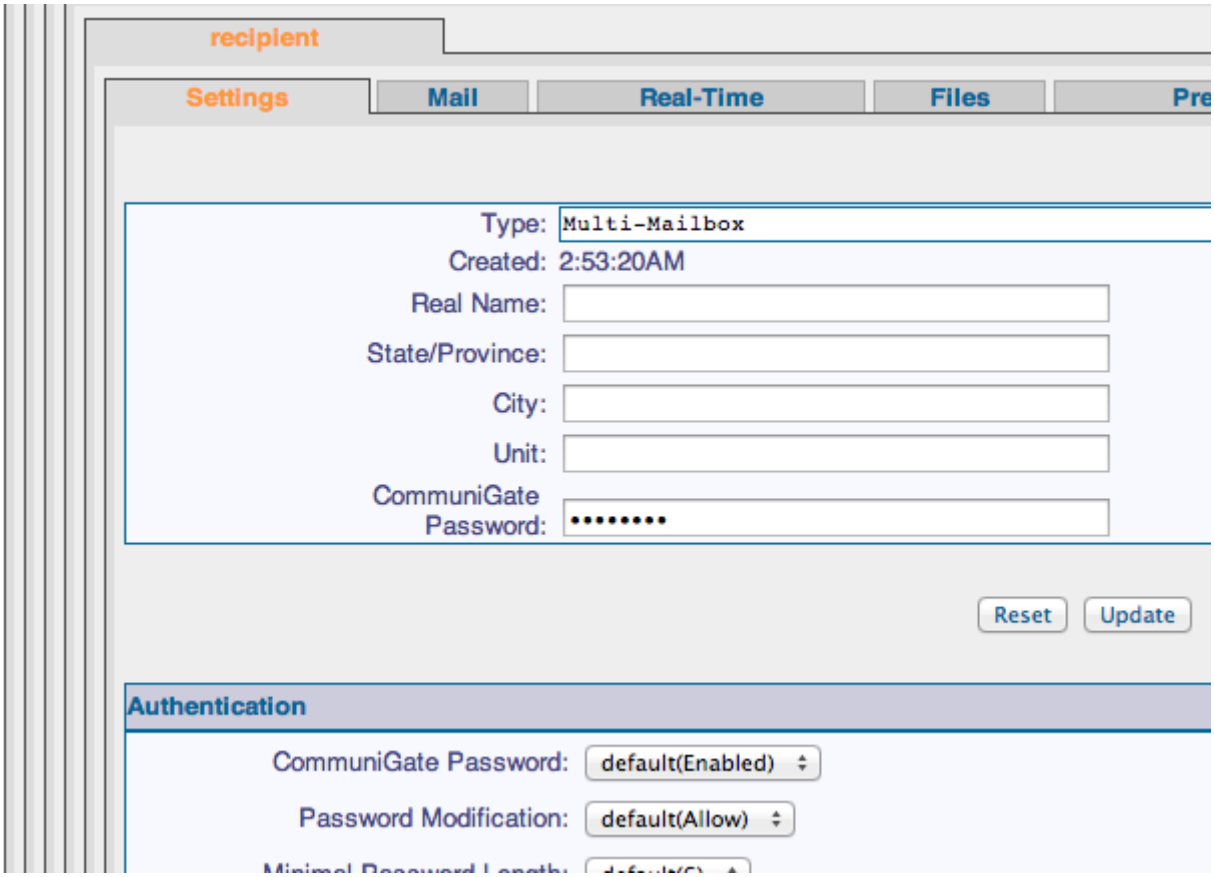
Продолжим настройку с того места на котором остановились в предыдущей статье. У нас уже установлен сервер и выбрано имя главного домена. Настало время завести пользователей. Заходим на страницу Users->Domains адмнки и выбираем главный домен:



В домене уже есть 2 служебных пользователя — postmaster — главный администратор и

pbx — техническая учетная запись от имени и с настройками которой запускаются голосовые приложения установленные по-умолчанию (подробнее о голосовых функциях расскажем в следующих статьях)

Создать нового пользователя легко — вводим имя, например recipient в текстовое поле возле кнопки «Create account» и нажимаем на нее. У вас откроется страница настроек нового пользователя, где можно будет ввести пароль для учетной записи — поле «Communigate password»:



Прием

Это самый трудоемкий по настройке раздел почты, связано это в первую очередь с борьбой со спамом. Мы, с одной стороны, не хотим принимать лишние письма (чтобы не прогонять слишком много писем через лексический спам фильтр, если он есть, да и просто лишний раз сервер не нагружать мусором), с другой — не хотим отказывать нормальным отправителям.

DNS

Хотя мы уже можем принять письма в только что созданные учетные записи, но необходимо будет использовать IP адрес в доменной части имени получателя. Это довольно неудобно для пользователей, поэтому все почтовые протоколы пользуются DNS.

Основным протоколом для доставки почты является SMTP, он используется как между серверами, так и от клиента к серверу (но не наоборот).

При этом процесс доставки письма от почтового клиента на сервер для отправки дальше мы будем называть регистрацией (submission) письма, а отправкой именно процесс доставки письма адресату (в случае SMTP адресаты находятся на других серверах).

Для полноценной работы этого протокола необходимы DNS записи типа MX. Они содержат три поля — имя почтового домена, приоритет и имя сервера обслуживающего домен. Для каждого имени сервера должна существовать DNS запись типа A.

Запись с наивысшим приоритетом считается основным почтовым сервером, а остальные — backup серверами.

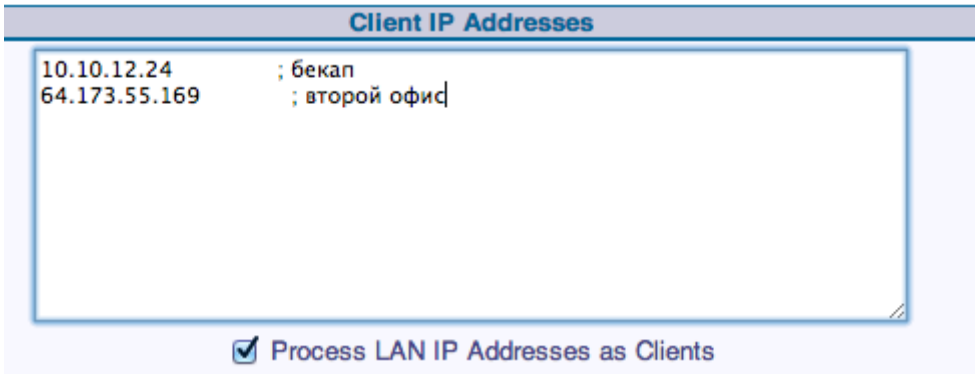
Например:

```
>nslookup -type=MX google.com

google.com      MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
google.com      MX preference = 10, mail exchanger = aspmx.l.google.com
google.com      MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
google.com      MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.com      MX preference = 40, mail exchanger = alt3.aspmx.l.google.com

aspmx.l.google.com      internet address = 74.125.143.26
alt1.aspmx.l.google.com internet address = 173.194.64.26
alt2.aspmx.l.google.com internet address = 74.125.142.26
alt3.aspmx.l.google.com internet address = 74.125.140.26
alt4.aspmx.l.google.com internet address = 173.194.74.26
```

Клиентские IP адреса (Client IPs)

В Communigate Pro существует понятие Клиентских адресов. По сути это доверенные IP адреса — они обычно имеют ряд привилегий по сравнению с обычными и в некоторых настройках отвечающих за безопасность можно выбирать значения «только для клиентов» и «для всех кроме клиентов».

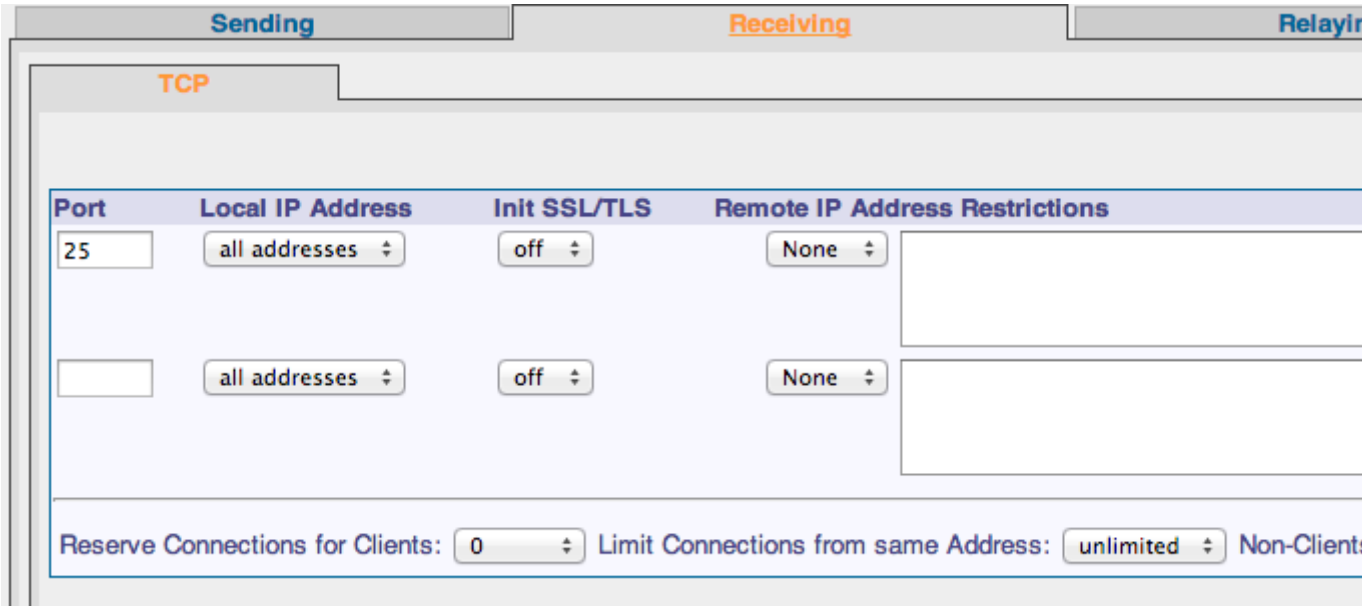
В админке CGPro клиентские адреса задаются полем типа «список адресов», этот тип поля активно используется и в других настройках (страница Setting->Network->Client IPs):



Приемники (Listeners)

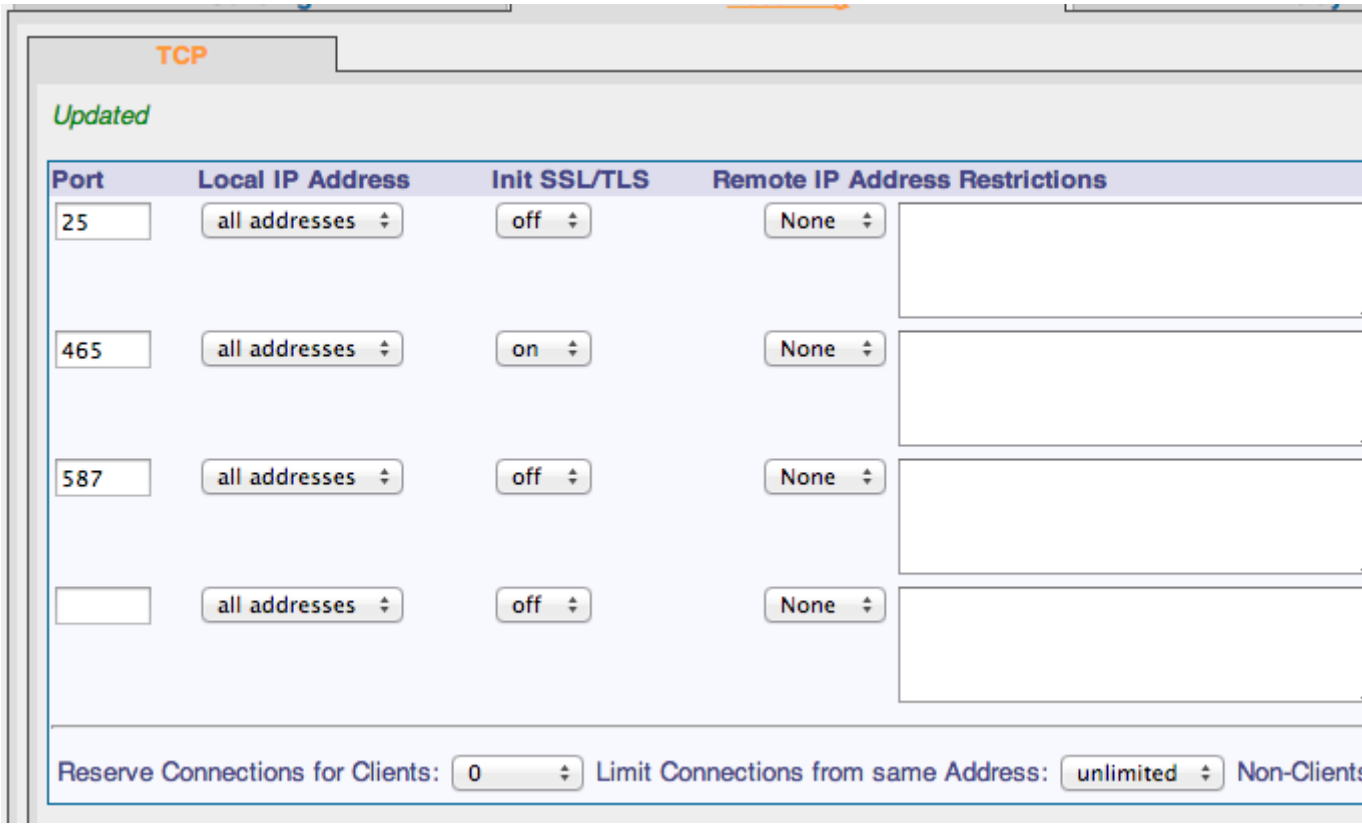
У каждого протокола, для которого Communigate Pro умеет принимать соединения есть свой список приемников (объекты сервера создающие сокеты), например SMTP (Settings-

>Mail->SMTP->Receiving->«Listener»):



Каждый приемник открывает сокеты на определенном порту и определенном IP адресе (это необходимо, чтобы CGPro мог стоять на одной машине, с Web сервером — web сервер занимает 80-й порт на одном IP, а CGPro на другом).

По умолчанию в SMTP модуле настроен только 25 порт, добавим сразу еще 2, положенных по стантарту:



В современной версии SMTP порт 25 предназначен в основном для серверов, клиенты же должны пользоваться 587-м, его отличие в обязательном использовании аутентификации через команду SMTP AUTH.

Protection

Существует множество протоколов помимо SMTP позволяющих зарегистрировать письмо на сервере, но все они работают с аутентификацией от имени одного из аккаунтов. SMTP в ряде случаев не может позволить себе такой роскоши, поскольку предназначен для получения писем от произвольных серверов.

Из-за этого есть ряд мер, которые необходимо предпринять, чтобы хоть немного усложнить жизнь спаммерам.

Релеинг

Релеинг это прием письма сервером, для пересылки его дальше адресату.

SMTP в принципе позволяет регистрировать письма предназначенные для сторонних серверов, но на практике такую возможность лучше закрыть для всех отправителей, кроме доверенных, так как если позволить пересылку на чужие сервера с IP адреса под контролем спаммеров, администраторы этих серверов скорее всего заблокируют все письма от вас.

Настройки релея находятся на странице <nobr/>Settings->Mail->SMTP->Relaying и значения по-умолчанию вполне оптимальны:

Главное не изменить их случайно или без конкретной причины.

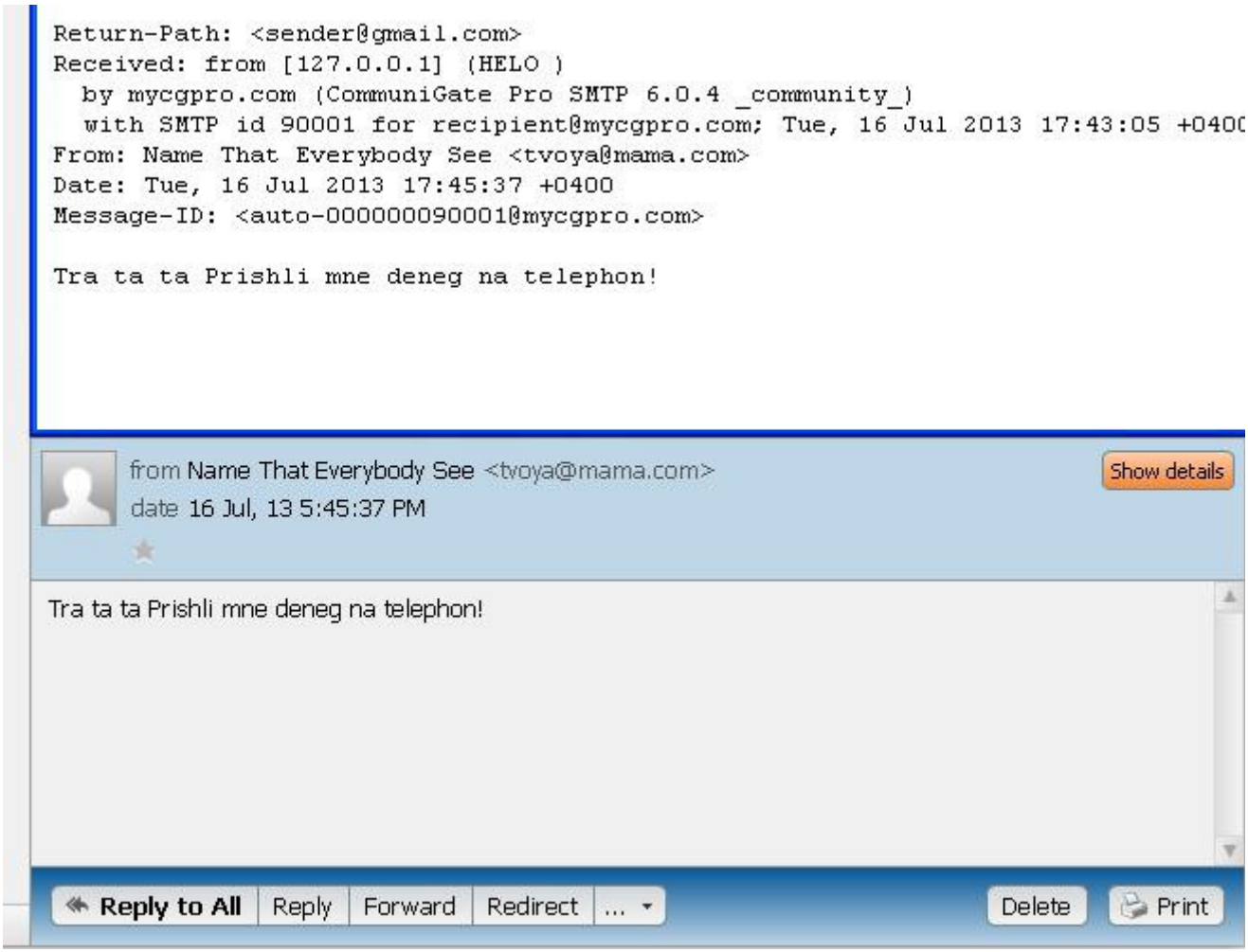
Проверки заголовков

Основными заголовками при получении SMTP письма являются отправитель и получатель. Рассмотрим пример SMTP сессии:

```
220 mycgpro.com ESMTP CommuniGate Pro 6.0.4 is glad to see you!
helo
250 mycgpro.com domain name should be qualified
Mail from:sender@gmail.com
250 sender@gmail.com sender accepted
rcpt to: recipient@mycgpro.com
250 recipient@mycgpro.com will leave the Internet
data:
```

```
354 Enter mail, end with "." on a line by itself
From: Name That Everybody See <tvoya@mama.com>

Tra ta ta Prishli mne deneg na telephon!
.
250 90001 message accepted for delivery
```

Тут отправитель задается командой MAIL FROM, а получатель RCPT TO. Самое главное, что должен знать администратор, это то, что поле которое показывается всеми без исключения почтовыми клиентами как «От кого» (заголовок «From» в письме) на самом деле является не отправителем, а просто частью тела письма. Большая часть проверок заголовков (включая популярные Remote BlackLists) работают именно с отправителем установленным командой протокола, а о теле письма понятия не имеют. В MIME формате отправителю соответствует поле «Return-path».



(Письмо полученное в SMTP сессии приведенной выше в MIME формате и интерфейсе)

Суть проверок «Return-path» в том, что при получении команды Mail From сервер извлекает доменную часть адреса и проверяет наличие этого домена в DNS. Есть также усиленная версия этой проверки — Reverse Connect, при использовании этой проверки, CGPro производит подключение к серверу отправителя и проверяет принимает ли этот сервер письма для отправителя с именем из команды Mail From.

Довольно популярной проверкой Return-path является SPF-проверка. Она требует DNS записей типа TXT специального формата, эти записи называют SPF записями. Они

содержат имя почтового домена и список IP адресов, которые являются легитимными отправителями писем с данной доменной частью. Например:

```
>nslookup -type=TXT google.com
google.com      text = "v=spf1 include:_spf.google.com ip4:216.73.93.70/31
ip4:216.73.93.72/31~all"
```

Основной минус этого способа — работает только с отправителями, администраторы серверов которых знают и используют эту проверку. В WebAdmin настройки приема почты собраны на одной странице Settings->Mail->SMTP->Receiving:

RBL и обычный blacklist рассматривать не будем так как эти типы проверок довольно известны (в основном из-за того, что многие люди из России и СНГ регулярно обнаруживают себя в них) и никаких сложностей по настройке быть не должно.

Обработка письма

При получении письма оно сразу начинает записываться на жесткий диск в папку Queue базовой директории с расширением .tmp. Как только процесс получения завершается расширение меняется на .msg и модуль принявший письмо ставит его в общую очередь.

При внезапной перезагрузке или отключении сервера письма из очереди (.msg файлы папки Queue) просто ставятся в нее заново.

Queue

В очередях письма зарегистрированные одними модулями ждут доставки в другие модули и\или в пользовательские ящики.

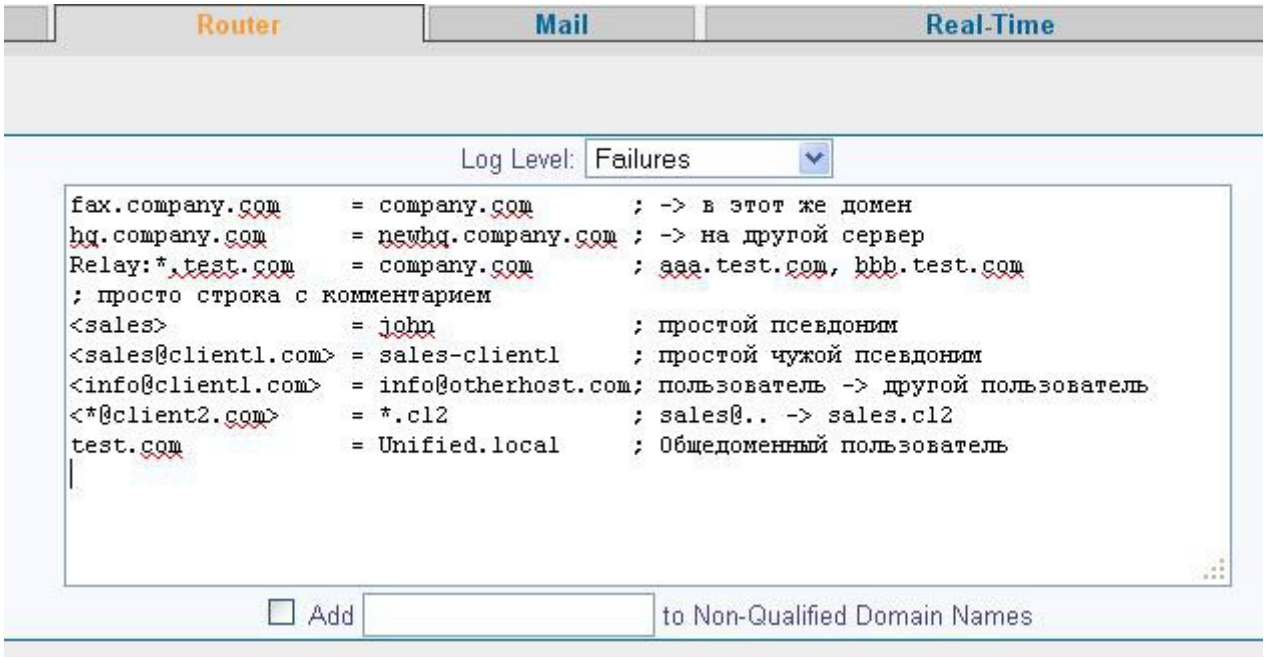
В очереди с письмом происходят следующие события:

- Анализ и преобразование адреса получателя.
- Применяем общесерверные правила.
- Файл очереди ставиться в одну или несколько логических очередей (в зависимости от того какие модули являются получателями письма)
- Применяем доменные или пользовательские правила
- Обработка писем в модулях-получателях.

Маршрутизатор(Router)

Каждый раз когда Communigate Pro сталкивается с почтовыми адресом он пропускает его

через модуль Router. У администратора, помимо вспомогательных средств управления роутингом письма (такие как правила, псевдонимы доменов и пользователей), есть мощный инструмент обеспечивающий удобный доступ непосредственно в процесс обработки адресов — таблица роутинга:



формат каждой строки в этой таблице:

[префикс релея:][префикс типа записи:]left=right[; комментарий]

Схема работы таблицы следующая — записи просматриваются по одной, начиная с верхней, если очередную удалось применить для преобразования адреса, то новый адрес подается на вход в модуль роутинга с самого начала.

По-умолчанию записи в таблице работают для адресов встречающихся во всех операциях и функциях сервера. Запись может также работать только для одного из 3 типов операций если отмечена соответствующим префиксом — «Mail», «Access» и «Signal».

Существует еще один тип префикса — «Relay». Если для какого-то получателя сработала запись с таким префиксом, то письмо получает специальную пометку и оно будет отправленно вне зависимости от того пришло оно от доверенного источника (с клиентского IP или от аутентифицированного пользователя) или нет. Это довольно опасная настройка, так как она позволяет спаммерам беспрепятственно отправлять письма на сервер на который у вас стоит перенаправление.

Логические очереди

Есть 4 вида очередей на отправку писем — на другие сервера (SMTP), в локальные ящики (LOCAL), в сторонние программы (PIPE) и в списки рассылки (LIST).

Каждая из этих очередей делится на несколько других. Например есть SMTP очередь на каждый домен — получатель, и есть LOCAL очередь на каждый аккаунт. Это позволяет

доставлять письма большими порциями — по многу писем за одно соединение или открытие почтового ящика.

Правила

Правила применяются в два подхода — в начале Серверные правила ко всем письмам (до постановки в очереди доставки), а потом Доменные и Пользовательские правила, но только для писем из очереди локальных ящиков LOCAL. Доменные правила с точки зрения внутреннего устройства абсолютно неотличимы от правил Пользователей, но применяются ко всем аккаунтам домена.

Подобная система применения правил означает, что Доменные и Пользовательские правила могут влиять только на входящие письма (исходящие письма в LOCAL очередь не попадают). То есть для выполнения каких-либо манипуляций над исходящими письмами подходят только Серверные правила.

Получение ящиков

Как и в случае с отправкой есть очень много протоколов, по которым можно получить содержимое ящиков хранящихся на сервере POP, IMAP, XIMSS, HTTP (AirSync, WebUser). Но получение ящиков практически всегда подразумевает аутентификацию клиента запрашивающего информацию.

Никаких особых настроек у этих протоколов нет — все должно заработать сразу «из коробки».

Имя пользователя в настройках клиентов желательно указывать полностью, включая доменную часть (если ваш клиент, как некоторые версии Outlook, автоматически отрезает доменную часть по символу '@' можно использовать '%' вместо него).

Подводим итоги

Мы рассмотрели самые важные настройки с которыми сталкивается начинающий администратор почты на Communigate Pro. В этой статье есть небольшой перекос в сторону настроек регистрации и отправки писем, связано это с тем, что такие обширные темы как Router и Правила тяжело уместить в рамки небольшой статьи. Рекомендуем ознакомиться с ними дополнительно в онлайн мануале:

Router eng \ rus
Правила eng1, eng2 \ rus1 , rus2