Communigate Pro

> **外國 language!**
>
> В статье используется несколько языков. Необходимо использовать один. Совсем неплохо, если это будет русский.

CommuniGate Pro — серверная платформа для организации электронной почты, передачи голосовых данных посредством технологии VoIP, мгновенного обмена сообщениями и автоматизации совместной работы. Программное обеспечение CommuniGate Pro поддерживает различные операционные системы и работает как в сетях IPv4, так и IPv6.

Содержание [убрать]

[9]

ЗАДАЧА

Создать полнофункциональную систему унифицированных коммуникаций (почта+телефония+IM) на 1500 человек с защитой от вирусов, спама и нежелательного контента, с возможностью обучения фильтра пользователями.

Описываемая система работает на базе операционной системы SLES10 SP2 (ppc64) [1] в логическом разделе LPAR [2] на сервере IBM pSeries [3]. Используется 32х-битная ppc-сборка CommuniGate Pro 5.4 [4].

ЛИЦЕНЗИРОВАНИЕ

Описание политики лицензирования CommuniGate Pro и сопутствующего ПО

УСТАНОВКА

Для начала следует удалить текущий почтовый пакет из системы. В SuSE Linux это делается через YaST, удаляемый пакет: ***postfix***

Communigate Pro

Следует помнить, что диск восстановления SUSE без вопросов меняет коммунигейтовский внутренний

sendmail, после чего перестают уходить во внешний мир письма из локальной очереди.

Последнюю версию communigate под различные аппаратные платформы можно взять на сайте производителя по адресу:ftp://ftp.stalker.com/pub/CommuniGatePro/

Установка из rpm-пакета:

```
cd /usr/local/src
wget ftp://ftp.stalker.com/Pub/CommuniGatePro/CGatePro-Linux.ppc.rpm
rpm -Uvh CGatePro-Linux.ppc.rpm
```

StartUp-скрипт

Startup скрипт Communigate Pro при установке в SUSE с VLAN's требует некоторой доработки.
Открываем **/etc/init.d/CommuniGate** и находим строчку:

```
Required-Start:
```

Меняем ее на:

```
Required-Start: network $named
```

Выполняем в консоли:

```
insserv -r CommuniGate
insserv CommuniGate
```

Все! Теперь при перезагрузках системы Communigate будет подхватывать ip-адреса VLAN's

Добавление suse-like стиля rc к стартовому скрипту comunigate

```
ln -s /etc/init.d/CommuniGate /usr/sbin/rcCommuniGate
```

CLI.pm

Скачиваем perl-библиотеку CLI.pm [5] с сайта http://www.stalker.com/CGPerl/CLI.pm в директорию /usr/local/lib и делаем символическую ссылку в /usr/lib/perl5/{version}

Следует помнить, что при обновлении communigate следует вручную скачать новую версию библиотеки!

ClamAV

К сожалению (или счастью) авторам неизвестны коммерческие антивирусы, работающие на платформе POWER5 (ppc64)

RPM-пакет для SUSE можно взять по адресу: http://download.opensuse.org/repositories/security/
(Бинарный пакет для архитектуры PPC в репозитории отсутствует, зато .src.rpm прекрасно компилируется):

```
rm /usr/src/packages/RPMS/ppc/clamav*
cd /usr/local/src
wget "http://download.opensuse.org/repositories/security/SLE_10/src/
clamav-0.96.1-28.1.src.rpm"
rpmbuild --nodeps --rebuild --target=ppc clamav-0.96.1-28.1.src.rpm
rpm -Uvh /usr/src/packages/RPMS/ppc64/clamav*
```

Запуск демона при старте системы:

```
cd /etc/init.d
insserv clamd
```

Установка ежечасных автоматических обновлений вирусных баз:

```
cd /etc/cron.hourly
ln -s `which freshclam` clamav-update
```

SpamAssassin

Установка через CPAN:

```
perl -MCPAN -e shell
install Mail::SpamAssassin
```

Дополнительно мы установили следующие модули:

```
HTML::Parser
Mail::SPF
IP::Country
```

```
Net::Ident
IO::Socket::INET6
IO::Socket::SSL
Mail::DKIM
LWP::UserAgent
HTTP::Date
IO::Zlib
Encode::Detect
```

Запуск демона при старте системы:

```
cd /etc/init.d
insserv spamd
```

Настройка автообновлений правил идентификации спама из репозитория spamassassin:

/etc/cron.hourly/sa-update

```
sa-update && rcspamd restart
```

Фильтр для совместной работы cgp+clamav+spamassasin

Внешний фильтр cgpav для Communigate: http://program.farit.ru/doc/cgpav-rus.html

Бесплатный Clamav, Kaspersky Anti-Virus (AVP), Sophos Anti-Virus, Trend Micro, Dr.Web и SpamAssassin внешний фильтр (плагин) для почтового сервера CommuniGate Pro. Используется для сканирования всех сообщений, которые проходят через почтовый сервер CommuniGate Pro www.stalker.com

```
tar xvfz cgpavXXX.tar.gz
cd cgpavXXX
./configure --with-antivirus=clamav --with-spamassassin=yes --with-cgpro_dir=/
var/CommuniGate
make && make install
```

По-умолчанию программа установится в каталог */var/Communigate*; конфигурационный файл - */var/Communigate/Settings/cgpav.conf*

Тестовый (лабораторный) вирус eicar

Описание находится по адресу: http://www.eicar.org/anti_virus_test_file.htm

Нам для работы необходим файл http://www.eicar.org/download/eicar.com Именно с его помощью мы в дальнейшем будем тестировать нашу почтовую систему.

НАСТРОЙКА

Модификация конфигурационных файлов

/etc/clamd.conf

```
PidFile /var/lib/clamav/clamd.pid
# Локальный сокет необходим для работы с cgpav
LocalSocket /var/lib/clamav/clamd-socket
# Пользователь, от которого работает демон
User vscan
# Так же необходимо разрешить использование дополнительных
# групп для того, чтобы демон имел необходимые права
# доступа к сообщениям в спулере communigate
AllowSupplementaryGroups yes
```

/etc/group

```
mail:x:12:vscan
```

Добавляет пользователя vscan дополнительно в группу mail, чтобы демон имел возможность работы с каталогами /var/Communigate

/var/CommuniGate/Settings/cgpav.conf

```
# Не уведомляем отправителя о вирусе
```

```
sender_notification = false
# ...а получателя уведомляем...
recipients_notification = true
# ... и администратора тоже
postmaster_notification = true
# оригинальные заголовки письма помогают выяснить
# от кого на самом деле пришел вирус
original_message_headers = true
clamd_socket = /var/lib/clamav/clamd-socket
enable_spamassassin = true
spam_scan_local = false
spam_action = addheaderall
spam_header = X-Spam-Flag: Yes
spam_level_header = true
extra_spam_action = none
spamassassin_socket_type = unix
spamassassin_socket = /var/run/spam
```

/etc/sysconfig/spamd

```
SPAMD_ARGS="-d -c -a -L --socketpath=/var/run/spam
```

CommuniGate

Все глобальные настройки осуществляются в административном веб-интерфейсе системы (http-порт 8010 или https-порт 9010 на почтовом сервере). Используется "экспертный" режим.

Настройки конкретных доменов, заведение и удаление пользователей производятся доменными администраторами из интерфейса управления домена: http://mail.example.com:8010/DomainAdmin/domain.name/

Изменение портов пользовательского web-интерфейса

По-умолчанию communigate предоставляет доступ к web-интерфейсу пользователя на портах 8100 и 9100. Изменим их на стандартные 80 и 443:

Установки -> Услуги -> HTTPU -> Приемник

Меняем 8100 на 80 и 9100 на 443

robots.txt / favicon.ico

Чтобы поисковые роботы не индексировали почтовую службу, создаем на локальной машине файл robots.txt [1] следущего содержания:

```
User-Agent: *
Disallow: /
```

Помещаем его в CommuniGate:

Пользователи -> Интерфейсы -> Загрузить файл

Теперь на запросы поисковых роботов cgp будет отдавать /robots.txt во всех доменах.

favicon.ico можно при желании загрузить таким же образом.

Подключение фильтра cgpav

Установки -> Общее -> Помощники

В разделе *Фильтрация Данных* добавляем правило с именем cgpav и пишем в *Путь к Программе*: cgpav

Теперь необходимо перейти в раздел: *Установки -> Почта -> Правила*

Добавляем правило с приоритетом 4, называем его *virus_scan* и нажимаем *Изменить*. Собираем правило:

- Данные - Размер письма
- Операция - Больше чем
- Параметр - 1024
- Действие - Внешний фильтр

- Параметр - cgpav

Нажимаем *Модифицировать*

В приведенном примере проверке подвергнутся и входящие и исходящие письма больше 1024 байт.

При желании можно исключить из проверки письма, приходящие из доверенных источников, к примеру с рабочих ПК предприятия, защищенных корпоративным антивирусом. В таком случае правило для подключения cgpav будет выглядеть следующим образом:

- Данные - Размер письма
- Операция - Больше чем
- Параметр - 1024
- Данные - Источник
- Операция - Не среди
- Параметр - trusted,authenticated
- Данные - Любой маршрут
- Операция - Среди
- Параметр - LOCAL(*,LIST(*
- Действие - Внешний фильтр
- Параметр - cgpav

В данном случае из проверки будут исключены письма отправленные из доверенных источников (локальные адреса, аутентифицированные пользователи) и письма, маршрутизируемые не в локальные аккаунты и списки рассылки [6].

Запрещение использования определенных типов файлов

Всвязи с трудоемкостью ручного добавления большого количества однотипных фильтров, была использована следующая схема: фильтры были сгенерированы sh-скриптом по шаблону, а получившийся результат вставлен в конфигурационный файл /var/CommuniGate/Settings/Rules.settings

Правило использует заголовки письма, вставляемые дополнительным скриптом *find-attachments.pl*

Скрипт *~/bin/generate.sh* для генерации правил:

```
#!/bin/bash

for i in ade adp bas cpl crt hlp inf ins isp lnk mdb mde msc msi msp mst pcd
reg sct shs url\
 vb wsc bat chm cmd com exe hta jse pif scr shb vbe vbs vbx wsf wsh asd dllocx
vxd 386 asp\
  asx bin cab cgi cil cpe cvp eml ex_ inp jar keyreg mda mdw mp3 nte nws pl pm
pot pps slb\
  swf swt sys vir vmx wms wmz xlw xms htr app csh fxp ksh mdt ops prg sh dot
adt btm cbt cla\
  clas class csc css drv email fon ini lib mht mhtm mhtml mso obj ov pgm smm
xlw xl cbl

do

echo "  ("
echo "    5,"
echo "    kill_attachment_$i,"
echo "    ((\"Header Field\", in, \"X-AttachExt: $i\")),"
echo "    ("
echo "      ("
echo "        \"Reject with\","
echo "        \"Error: \\\".$i\\\" file attachment types not allowed\e\e\""
echo "      )"
echo "    )"
echo "  ),"
done
```

Запрет на письма без темы или с бессмысленным бредом вместо нее

Если есть необходимость воспитания компьютерной грамотности своих пользователей техническими методами, можно осуществить это следующим образом.

Переходим в раздел: *Установки -> Почта -> Правила*

Добавляем правило с приоритетом 6, называем его *reject_out_emptysubj* и нажимаем *Изменить*. Собираем правило:

- Данные - Источник
- Операция - Среди
- Параметр - trusted,authenticated
- Данные - Тема
- Операция - Равно
- Параметр -
- Действие - Отвергнуть с
- Параметр - Messages without subject are not allowed here!

Нажимаем *Модифицировать*

Добавляем правило с приоритетом 6, называем его *reject_out_stupidsubj* и нажимаем *Изменить*. Собираем правило:

- Данные - Источник
- Операция - Среди
- Параметр - trusted,authenticated
- Данные - Тема
- Операция - Среди
- Параметр - 1,2,3,4,5,6,7,8,9,123,1234,12345,qwerty
- Действие - Отвергнуть с
- Параметр - Messages with stupid subject are not allowed here!

Нажимаем *Модифицировать*

Создание сертификатов для защищенного ssl-соединения

По умолчанию Communigate использует тестовый метод ssl-авторизации. Для обеспечения нормальной работы ssl необходимо внести следующие правки: В административном интерфейсе Communigate выбираем следующую вкладку:

Пользователи -> Домены -> Домен -> Безопасность -> SSL/TLS

И в окне "Услуги PKI криптографии" меняем значение на "включено". Далее необходимо сгенерировать самоподписанный сертификат во внутреннем генераторе сертификатов.

Следует помнить, что имя-идентификатор сертификата должен соответствовать точному dns-имени сервера, на который заходят пользователи вашего домена.

Защита от DoS атак

Чтобы предотвратить появление ситуации типа "отказ в обслуживании", вызваные черезмерным количеством одновременно открытых tcp-сессий используются следующие параметры:

"Установки" -> "Почта" -> "SMTP" -> "Прием"

Устанавливаем параметр "Каналы" на значение 1000. Переходим по ссылке "Приемник" и устанавливаем параметры:

- Ограничение на соединения с одного Адреса -> 100
- Резерв соединений для Клиентов -> 300

Порт Submission (587)

Для клиентов, находящихся вне локальной сети предприятия, следуя RFC 2476 рекомендуется открыть порт 587 (Submission) [7] [8] на сервере и настроить почтовые клиенты на работу с SMTP с этим портом, вместо 25го, который все больше и больше провайдеров закрывают в своих сетях для борьбы со СПАМом.

Установки -> Почта -> SMTP -> Прием -> Приемник

- Добавляем порт **587**
- Начальный SSL/TLS вкл.

Порт POP-SSL (995)

Для клиентов которые очень хотят работать по pop3

Установки -> Доступ -> POP -> Приемник

- Добавляем порт **995**
- Начальный SSL/TLS вкл.

Pronto!

В версии 5.3 в интерфейсе Pronto! появилась очень удобная кнопочка "Обратная связь", открывающая новое письмо с адресом получателя**pronto-feedback@communigate.com**. Логично заменить его на e-mail адрес своей техподдержки. Заходим в каталог*/opt/CommuniGate/WebSkins/Pronto-* (обратите внимание на "-" на конце) и выполняем следующую команду:

```
find ./ -type f -name "*.data"| xargs perl -pi -w -e 's/pronto-feedback
\@communigate.com/support\@example.com/g;'
```

Локальные вспомогательные скрипты

Данные скрипты установлены в директории /usr/local/cgpro-scripts и имеют сиволические ссылки в /usr/local/bin Они помогут автоматизировать множество операций с почтовой системой.

- **spamassasin_spam_learner**

Скрипт для автоматического обучения байесовского фильтра spamassassin со специальных аккаунтов *learn-spam* и *learn-ham*. Скрипт имеет символическую ссылку в */etc/cron.daily*

```
#!/bin/bash

# Learn SPAM:
/usr/bin/sa-learn --showdots --mbox --spam /var/CommuniGate/Accounts/learn-
spam.macnt/INBOX.mbox
/usr/bin/sa-learn --showdots --mbox --spam /var/CommuniGate/Accounts/learn-
spam.macnt/SPAM.mbox

# Learn HAM:
/usr/bin/sa-learn --showdots --mbox --ham  /var/CommuniGate/Accounts/learn-
ham.macnt/INBOX.mbox
/usr/bin/sa-learn --showdots --mbox --ham  /var/CommuniGate/Accounts/learn-
ham.macnt/SPAM.mbox

# Rebuild bayes DB
sa-learn --sync --force-expire

# Kill all letters older than 1 day:
/usr/local/bin/oldmail_del.pl
```

- **oldmail_del.pl**

Скрипт, используемый в связке с spamassasin_spam_learner, удаляет письма старше одного дня.

- **findattach-cgp**

Усовершенствованная версия программы для поиска приложений в письмах, написанная на языке C

Исходник забираем со следующего сайта: http://kocmuk.ru/tag/findattach/ Для работы приложения необходимы библиотеки GNU Mailutils версии не ниже 2.2, берем с официального сайта: http://www.gnu.org/software/mailutils/

После сборки и установки Mailutils компилируем статически findattach-cgp.c:

```
gcc -Wall -I  /%path-to-mailutils-distrib%/include/ -pthread -lcrypt
findattach-cgp.c /%path-to-mailutils-distrib%/mailbox/.libs/libmailutils.a -o
findattach-cgp
```

и кладем получившийся бинарник в /usr/local/bin.

Подключение фильтра происходит следующим образом:

Установки -> Общее -> Помощники

В разделе *Фильтрация Данных* добавляем правило с именем Find_Attachments и пишем в *Путь к Программе* в нашем случае:

```
/usr/local/bin/findattach-cgp -f
```

Ключ "-f" включает режим т.н. fuzzy-logic, определяющий тип вложения, если то не содержит расширения.

Теперь необходимо перейти в раздел: *Установки -> Почта -> Правила*

Добавляем правило с приоритетом 6, называем его *Find_Attachments* и нажимаем *Изменить*. Собираем правило:

- Данные - Размер письма
- Операция - Больше чем
- Параметр - 2048
- Действие - Внешний фильтр
- Параметр - Find_Attachments

Нажимаем *Модифицировать*

- **find-attachments.pl**

Скрипт для поиска вложений в письмах и добавления специального заголовка, используется соввместно с фильтрами communigate

Подключение фильтра происходит следующим образом:

Установки -> Общее -> Помощники

В разделе *Фильтрация Данных* добавляем правило с именем Find_Attachments и пишем в *Путь к Программе*:"путь к инрерптитатору perl + путь к скрипту" (в нашем случае: */usr/bin/perl /usr/local/bin/find-attachments.pl*)

Теперь необходимо перейти в раздел: *Установки -> Почта -> Правила*

Добавляем правило с приоритетом 6, называем его *Find_Attachments* и нажимаем *Изменить*. Собираем правило:

- Данные - Размер письма
- Операция - Больше чем
- Параметр - 2048
- Действие - Внешний фильтр
- Параметр - Find_Attachments

Нажимаем *Модифицировать*

- **auto-delite-junk.pl**

Скрипт для автоматического удаления писем из папки SPAM старше 14 дней

- **AddFilter.pl**

Скрипт для автоматической настройки аккаунтов пользователей, добавляет каждому папку SPAM и правило, складывающее туда письма, помеченные spamassassin флагом X-Spam-Flag: Yes

Антиспамерские меры

CommuniGate

Задержка ответа сервера

Установки -> Почта -> SMTP -> Прием

В разделе ограничения: отложить ответ сервера на 7 сек.

Время задержки можно варьировать, однако мы не рекомендуем устанавливать задержку более, чем на 30 сек. несмотря на то, что по требованиям RFC задержка может составлять до 5 минут.

SPF проверка [9]

Установки -> Почта -> SMTP -> Прием

Проверять SPF-записи: Включено

Ограничения

Установки -> Почта -> SMTP -> Прием

Отсоединить после: **15** ошибок и Заблокировать Доступ на: **60 мин.**

Встречное соединение

Установки -> Почта -> SMTP -> Прием

Соединяться навстречу: Всегда

Так же возможно использования режима:

Соединяться навстречу: Добавлять поле

Режим "всегда" может привести к некорректной работе с серверами, использующими серые списки (greylisting) или внешние релеи для отправки почты. Добавляемые поля можно использовать при обработке spamassassin. Однако же при регулярном контроле лог-файлов режим "всегда" может быть использован, поскольку резко сокращает поток нежелательной корреспонденции.

Неиспользуемые (в настоящее время) значения полей:

```
X-Reverse-Check: Bad SMTP prompt at the host
```

Используемые значения полей:

```
X-Reverse-Check: address rejected with reverse-check
X-Reverse-Check: connection closed by peer
X-Reverse-Check: connection refused
X-Reverse-Check: no relay available
X-Reverse-Check: no response
X-Reverse-Check: read time-out
X-Reverse-Check: reverse check protocol error
```

Блокировки RFC Reader

Идем: Установки -> Почта -> RFCReader

Ставим правила, отклоняющие письма с pipe:

```
From: *<*|*@*>
From: *|*
Return-Path: *<|*@*>
Return-Path: *|*
```

Блокированные Сетевые Адреса

Установки -> Сеть -> Блокировки

```
; непонятный sip-спаммер
92.243.14.140
; descr:          OJSC Uralsvyazinform, Khanty-Mansiysk department
; descr:          For ADSL users
; country:        RU
90.150.32.0-90.150.47.255
; netname:        IS-Stafraen-Dreifing
; descr:          BTnet xDSL (via Netheimur/XNet)
; country:        IS
81.15.51.0-81.15.51.255
; Hijacked IP space for spammers, see google or slashdot
134.17.0.0-134.17.255.255
; netname:        KYBERNA-NET
; descr:          Dialin connector ip SDSL customers
88.82.103.0-88.82.103.255
; ADSL-CONNECTION-FIXIP
; remarks:      please send ABUSE complains to abuse@bezeqint.net
62.219.224.0-62.219.239.255
; netname:      SURTECH-PH
```

```
; country:      PH
; descr:        Surtech Philippines Inc
203.131.110.168-203.131.110.175
; netname:        B-ONE-NET
; descr:          One.com A/S
195.47.247.0-195.47.247.255
200.223.236.0-200.223.236.31
; generic ip's
58.140.121.239
212.150.181.58
211.226.197.165
220.225.224.4
89.239.140.54
84.22.142.140
217.145.194.104
69.10.44.198
68.16.247.24
89.189.128.245
82.179.222.9
77.223.95.84
209.62.55.82
74.55.237.114
67.43.10.51
62.42.230.12
80.243.7.117
86.55.81.251
201.41.156.6
193.222.191.154
122.217.190.101
82.114.103.10
190.40.16.227
195.239.212.46
189.74.80.220
190.67.249.69
85.105.133.115
58.8.170.242
92.244.41.105
208.36.224.25
```

Использование блокировок по DNS-именам

В административном интерфейсе Communigate открываем следующую вкладку:

Установки -> Сеть -> Блокировки

Включаем "Вычислять Блокированные по DNS-именам". Мы используем следующие поля общего вида:

```
*.adsl.*
*.dsl.*
*.xdsl.*
*.pool.*
*.cable.*
*.dial.*
*.dip.*
*.adsl-dhcp.*
*.dynamic.*
*.pppoe.*
*.cable-modem.*
*.dsl-nat.*
*.broadband*.*
*.adsl-access.*
*.*.*.*.*.*
*-*-*-*-*.*
host-*.*.*
*.unused-addr.*
```

```
*.pppool.*
ppp-*.*.*
*gprs.*.*
*.dhcp.*
*.ppp.*
pppoe-*
adsl-*
dsl-*
*-homeuser-*.*.*
dynamic-*.*.*
bredband.*.*.*
broad.*.*.*
catv.*.*.*
cdma*.*.*
client.*.*.*
dlup.*.*.*
dslam.*
dyndsl.*
modem.*
*.ftth.*
*.ddns.*
*.in-addr.*.*
*-xdsl-dynamic.*
pptp.*
*.dsl-dynamic.*
*.xdsl-line.*
unnasigned-reverse-*
sdn.*.*.*
wdsl.*
wifi.*.*.*
wlan.*.*.*
```

Поля по конкретным операторам:

```
*.dyn.optonline.net
*.setardsl.aw
*.dsl-verizon.net
*.rima-tde.net
user.*.satfilm.net.pl
*.inturbo.lt
*.fios.verizon.net
pool-*.verizon.net
adsl*.etb.net.co
*.rdsnet.ro
adsl*.simnet.is
real-*.kvidex.ru
*.business.telecomitalia.it
cust-*.ontelecoms.gr
*.web2k.net
*.adslplus.ch
*.cl.metrocom.ru
*.Home-Lan.fastnet.lv
*.ttnet.net.tr
*.access.telenet.be
*.rr.com
*.users.intility.com
*.cableonda.net
*.netspace.net.au
*.cablesurf.de
*.customer-*.uninet-ide.com.mx
*.tukw.qwest.net
host*.gudzonserver.com
*.v.shared.ru
```

```
*.interlain.lv
*.cbcast.com
*.b-one.net
*.websiteactive.com
clt-*.vdnet.lt
*.giga-dns.com
*.netverk.com.ar
*.telecom.net.ar
*.btc-net.bg
*.net.upc.cz
*.client*.youtele.com
dyn*.pacific.net.sg
host*.butovo.com
homeuser*.perm.ru
*.isp.belgacom.be
*.cpe.netcabo.pt
*.ewe-ip-backbone.de
*.dyn.centurytel.net
*-*.*.cn.ru
*-*.wispnet.net
*.onocable.ono.com
*.cablep.bezeqint.net
*.cgocable.net
*.fibertel.com.ar
*.internetdsl.tpnet.pl
*.shawcable.net
*.asm.bellsouth.net
*.abo.wanadoo.fr
*.charter.com
*.*.fairgamemail.us
*.*.virtua.com.br
*.ad.jp
*.asianet.co.th
*.customer.alfanett.no
*.maxonline.com.sg
*.telpol.net.pl
*.user.veloxzone.com.br
*dynip.superkabel.de
*homenet.master.ru
*yahoobb.*.bbtec.net
*.bb.sky.com
*.bdsl.sk
*.bsb.vectranet.pl
*.claranet.co.uk
*.elb.vectranet.pl
*.customers.tvtnet.ch
*.sbcis.sbc.com
*.turktelekom.com.tr
*.uninet.lv
*.versanet.de
*.wanadoo.co.uk
a.*.sub.*.net.*.udm.net
b-internet.*.snt.ru
*.cust.bluewin.ch
*.lan.sify.net
*.is.co.za
client-*.*.satelnet.ro
*.fbx.proxad.net
duser-*-*.popnet.sk
dxb-*.alshamil.net.ae
host.*.rusmedia.ru
kabelnet-*-*.juropnet.hu
```

```
leased-line-*.telecom.by
*.comcast.net
nat-altair.*.netbynet.ru
nn.*.excitenetwork.com
p*-*.cust.nbox.cz
p*.mp*.aaanet.ru
p-.*.powernet.bg
public-gprs*.centertel.pl
customer-*.millicom.com
*.hkcable.com.hk
net*.omskdom.ru
*.live.blueyonder.co.uk
*.dsl-w.verizon.net
kns-*.kansstel.ru
*.pools.arcor-ip.net
*.uio.satnet.net
net*.e-kirov.ru
CLIENT-*.dialog.net.pl
*.fastportnet.cz
customers-*.dnet.dp.ua
free-*.net1.bg
segment-*.sify.net
*.sovintel.spb.ru
*.redes.acens.net
pc-*.vtr.net
*.dyn.*.awesomenet.net
*.optusnet.com.au
*.tlt.ru
cust-*.tsnet.ru
*-dsl.qfast.net
*.speedy.telkom.net.id
station*.unionjv.ru
koel-*-*.koelnet.com
bd*.virtua.com.br
node*-*.network.is.nl
*.comcastbusiness.net
*.wlan.rz.tu-bs.de
ppp*-*.global-ts.ru
cblmdm*.buckeyecom.net
*.hsi.kabelbw.de
*-dynamic.*.telecomitalia.it
*.ll.kw.ua
public*.cdma.*
user-*.msk.pl
*.codetel.net.do
dsl*.ttnet.net.tr
cable-*.blue-cable.de
*-*.rev.gaoland.net
cliente-*.iberbanda.es
*.onlinehome-server.com
*.retail.ttk.ru
vh*.hoster.by
host*.*.prov.ru
host*.tijo.3s.pl
*.ketnet.cz
*.digiweb.com.br
ns*.ovh.net
rps*.ovh.net
*.bereopelos.ru
ks*.kimsufi.com
*.cvdnet.pl
```

Так же при желании можно добавить строку вида

- (host name is unknown)

для того, что бы заблокировать все сетевые адреса которые не имеют обратных (PTR) записей в DNS [10] (отсутствие PTR является нарушением Секции 2.1 RFC 1912 и Секции 3.6 RFC 2821)

Использование блокирующих DNS-Серверов (RBL)

В административном интерфейсе Communigate открываем следующую вкладку:

Установки -> Сеть -> Блокировки

Включаем "Использовать Блокирующие DNS-Сервера (RBL)" и записываем адреса днс в графы. Мы используем следующие адреса:

- zen.spamhaus.org [11]
- cbl.abuseat.org [12]
- dul.ru [13]
- insecure-bl.rambler.ru [14]

Устанавливаем значение "Блокировать" в разделе "Письма с Блокированных Адресов"

Неблокируемые Адреса (Белые Дыры)

```
; mail.rustest.ru
213.79.68.66
; mail.belkult.ru (no PTR)
82.151.110.147
; mail.tspu.tula.ru (no PTR)
94.25.83.201
; mx1.vspu.ru (no PTR)
83.167.86.3
; ns.vgta.vrn.ru (no PTR)
93.88.139.1
; csr.csrs.ru (no PTR)
77.108.127.27
; post.rsreu.ru (no PTR)
82.179.89.3
; LiveJournal
208.93.0.128
208.93.0.50
; mail.zhivagobank.ru (no PTR)
95.83.158.20
; aeroflot.ru (bad reverse-check behavior)
89.208.33.137
```

Неблокируемые по DNS-именам

Установки -> Сеть -> Блокировки

Включаем "Вычислять Неблокируемые по DNS-именам"

```
*.edu
*.edu.ru
*.edu.cn
*.gov.ru
*.gov
*.amazon.com
*.freshmeat.net
*.intel.com
*.gmail.com
*.gnu.org
*.mail.ru
*.yandex.ru
*.mail.yandex.net
*.rambler.ru
*.subscribe.ru
*.ibm.com
```

```
*.hotmail.com
*.sotcom.ru
*.ryazan.su
*.ryazan.ru
*.novell.com
*.sun.com
*.livejournal.com
*.vkontakte.ru
*.pochta.ru
*.udsu.ru
*.rsr-online.ru
*.post.rzn.ru
*.nsu.ru
*.mac.com
*.rustest.ru
*.nnm.ru
*.icq.com
*.neweurasia.ru
*.ministry.ru
*.zhivagobank.ru
*.prometeus.ru
*.mgimo.ru
*.vspu.ru
*.google.com
*.cisco.com
*.goethe.de
*.goethe.org
*.msu.ru
*.masterbank.ru
*.gapm.ru
*.mfpa.ru
*.mpsinst.ru
*.yahoo.com
*.pinro.ru
*.sunrav.ru
*.vgta.vrn.ru
*.rosim.ru
```

Использование механизма SpamTrap

Также к дополнению к предыдущим методам, можно использовать Spamtrap. Communigate Pro имеет встроенный механизм "ловушек для спама", который заключается в создании нескольких ящиков-переадресаторов на специальный служебный адрес "spamtrap". Письма, приходящие на этот ящик будут автоматически распознаваться как спам и удаляться из всех аккаунтов пользователей. Для эффективной работы этого механизма стоит размещать ссылку на этот адрес на тех же ресурсах, где находятся реально существующие ящики пользователей, чтобы спам-боты индексировали их одновременно.

При наличии пары-тройки лишних доменов можно указать пересылать почту для неизвестных на spamtrap'ы. Это позволяет эффективно блокировать спамеров, подбирающих почтовые ящики пользователей по словарям.

Посмотреть на какие spamtrap'ы приходит больше всего писем можно командой:

```
grep spamtrap /var/CommuniGate/SystemLogs/*.log | awk '{ print $11; }' | sort | uniq -c | sort -n -r | head
```

SpamAssassin

Набор правил для русскоязычного спама: http://sa-russian.narod.ru/

Качаем и кладем в каталог:

```
/var/lib/spamassassin/<ver>/updates_spamassassin_org/
```

Первоначальный тюнинг

По совету из конфигурационного файла cgpav.cfg ставим следующий параметр:

```
score MIME_MISSING_BOUNDARY 0
```
Необходимость отключения данной проверки вызвана тем, что cgpav обрезает большие письма до 50K (по-умолчанию) перед передачей фильтру spamassassin, что приводит к ложному срабатыванию и, иногда, ложной классификацией писем со вложениями в качестве спам-сообщений.

Добавим больше доверия прошедшим spf-проверку

```
score SPF_PASS -2.0
```
Auto-whitelist

Настраиваем auto_whitelist, что в терминологии spamassassin означает, что будут высчитываться средние оценки для отправителя.

В коносли делаем следущее:

```
mkdir /etc/mail/spamassassin/auto-wl/
chmod 777 /etc/mail/spamassassin/auto-wl/
touch /etc/mail/spamassassin/auto-wl/auto-whitelist
chmod 666 /etc/mail/spamassassin/auto-wl/auto-whitelist
```
Прописываем в конфигурационном файле:

```
auto_whitelist_path        /etc/mail/spamassassin/auto-wl/auto-whitelist
auto_whitelist_file_mode   0666
```
Если что-то неправильно с правами доступа, то в файле /var/log/mail появятся такие строчки:

```
mail spamd[582]: auto-whitelist: open of auto-whitelist file failed: auto-
whitelist:
cannot open auto_whitelist_path /etc/mail/spamassassin/auto-wl/auto-whitelist:
Permission denied
```
Исключения для рассылок и важных доменов

```
whitelist_from  *@rustest.ru
whitelist_from  *@neweurasia.ru
whitelist_from  *@mac.com
whitelist_from  *@staff.mesi.ru
whitelist_from  *@transtk.ru
whitelist_from  *@col.ru
whitelist_from  *@rsr-online.ru
whitelist_from  *@post.rzn.ru
whitelist_from  *@zhivagobank.ru
whitelist_from  *.sovcombank.ru
whitelist_from  *@bti.secna.ru
whitelist_from  *@rcic.altai.ru
whitelist_from  *.nsu.ru
whitelist_from  *@sgu.ru
whitelist_from  *@dspl.ru
whitelist_from  *@csu.ru
whitelist_from  *@psu.ru
whitelist_from  *@vsu.by
whitelist_from  *@sgap.ru
whitelist_from  *.rsu.ru
whitelist_from  *.udsu.ru
whitelist_from  *@ministry.ru
whitelist_from_rcvd *@rsu.edu.ru rsu.edu.ru
whitelist_from_rcvd *@rspu.ryazan.ru rsu.edu.ru
whitelist_from_rcvd *@ttc.ryazan.ru rsu.edu.ru
whitelist_from_rcvd *@www.rsu.edu.ru rsu.edu.ru
whitelist_from_rcvd *@proxy.rsu.edu.ru rsu.edu.ru
whitelist_from_rcvd *@me.com mac.com
whitelist_from_rcvd *@russia.ru post.russia.ru
whitelist_from_rcvd *@subscribe.ru subscribe.ru
whitelist_from_rcvd *@sura.ru mail.sura.ru
whitelist_from_rcvd *@uni.udm.ru udsu.ru
whitelist_from_rcvd *@rsreu.ru post.rsreu.ru
whitelist_from_rcvd *@novell.com novell.com
```

```
whitelist_from_rcvd *@163.com 163.com
whitelist_from_rcvd *@pcweek.ru skpress.ru
whitelist_from_rcvd *@sfpgu.ru mail.sfpgu.ru
whitelist_from_rcvd *@aitek.ru aitek.ru
whitelist_from_rcvd *@center.rt.ru centertelecom.ru
whitelist_from_rcvd *@centrettc.ru centrettc.ru
whitelist_from_rcvd *@mtt.ru mtt.ru
whitelist_from_rcvd *@unicreditgroup.ru unicreditgroup.ru
whitelist_from_rcvd *@nlink.ru nlink.ru
whitelist_from_rcvd *@iptechs.ru nlink.ru
whitelist_from_rcvd *@eletek.ru eletek.ru
whitelist_from_rcvd *@mail.zakazrf.ru mail.zakazrf.ru
whitelist_from_rcvd *@icloud.com me.com
whitelist_from_rcvd *@dropbox.com dropbox.com
whitelist_from_rcvd *@min-obr.ru sweb.ru
whitelist_from_rcvd *@mail.ryazan.ru mail.ryazan.ru
whitelist_from_rcvd *@pinro.ru pinro.ru
whitelist_from_rcvd *@mail.ru mail.ru
whitelist_from_rcvd *@list.ru mail.ru
whitelist_from_rcvd *@bk.ru mail.ru
whitelist_from_rcvd *@yandex.ru yandex.ru
whitelist_from_rcvd *@narod.ru yandex.ru
#whitelist_from_rcvd *@rambler.ru rambler.ru
whitelist_from_rcvd *@gmail.com google.com
whitelist_from_rcvd *@vimeo.com smtp.vimeo.com
#whitelist_from_rcvd *@hotmail.com hotmail.com
whitelist_from_rcvd *@yahoo.com yahoo.com
whitelist_from_rcvd *@netapp.com netapp.com
whitelist_from_rcvd *@lists.sourceforge.net lists.sourceforge.net
whitelist_from_rcvd *@sunrav.ru kyoto.hostforweb.net
whitelist_from_rcvd *@vgta.vrn.ru vgta.vrn.ru
whitelist_from_rcvd *@zhivagobank.ru mail.zhivagobank.ru
whitelist_from_rcvd *@mail.zhivagobank.ru mail.zhivagobank.ru
whitelist_from_rcvd *@mx.ru mx.demos.su
whitelist_from_rcvd *@is-mon.ru is-mon.ru
whitelist_from_rcvd *@gzgu.ru mail.mgapi.ru
whitelist_from_rcvd *@informika.ru informika.ru
whitelist_from_rcvd *@lists.wikimedia.org lists.wikimedia.org
whitelist_from_rcvd *@forest.ru mail.forest.ru
whitelist_from_rcvd *@biodiversity.ru mail.biodiversity.ru
whitelist_from_rcvd *@assist.ru smtp.assist.ru
whitelist_from_rcvd *@elibrary.ru elibrary.ru
whitelist_from_rcvd *@megaplan.ru megamonstr.megaplan.ru
whitelist_from_rcvd *@zakupki.gov.ru zakupki.gov.ru
whitelist_from_rcvd *@megafoncenter.ru mail.megafoncenter.ru
```

Правила для проверки результатов встречного соединения (reverse connect)

/etc/mail/spamassassin/local.cf

```
header REV_CHECK_DROPPED X-Reverse-Check =~ /connection closed by peer/
describe REV_CHECK_DROPPED Reverse check connection of sender mail address
closed by remote server
score REV_CHECK_DROPPED 4

header REV_CHECK_FAILED X-Reverse-Check =~ /address rejected with reverse-
check/
describe REV_CHECK_FAILED Reverse check of sender mail address rejected by
remote server
score REV_CHECK_FAILED 4.5

header REV_CHECK_NORELAY X-Reverse-Check =~ /no relay available/
describe REV_CHECK_NORELAY No relay available for reverse check
score REV_CHECK_NORELAY 4.5
```

```
header REV_CHECK_NORESP X-Reverse-Check =~ /no response/
describe REV_CHECK_NORESP No response from remote server to reverse check of
sender mail address
score REV_CHECK_NORESP 4

header REV_CHECK_PROTOERR X-Reverse-Check =~ /reverse check protocol error/
describe REV_CHECK_PROTOERR Reverse check protocol error on remote server
score REV_CHECK_PROTOERR 4

header REV_CHECK_REFUSED X-Reverse-Check =~ /connection refused/
describe REV_CHECK_REFUSED Reverse check of sender mail address refused by
remote server
score REV_CHECK_REFUSED 4.5

header REV_CHECK_TIMEOUT X-Reverse-Check =~ /read time-out/
describe REV_CHECK_TIMEOUT Reverse check of sender mail address timed out
score REV_CHECK_TIMEOUT 4
```

DNSWL

При желаниии можно включить данный сервис

Сервис DNSWL [15] представляет собой т.н. анти-rbl: список известных легитимных почтовых серверов. Сервис используется для уменьшения процента ложных срабатываний при обработке почты анитиспам-фильтрами. Сервера интернета делятся на 4 зоны:

- High никогда не пересылали спам
- Medium черезвычайно редкие спам-рассылки, быстро реагируют
- Low изредка рассылают спам, реагируют в приемлимое время
- None легитимные сервера, которые кроме писем так же могут рассылать спам

Модификация **/etc/mail/spamassassin/local.cf**:

```
header __RCVD_IN_DNSWL          eval:check_rbl('dnswl-firsttrusted',
'list.dnswl.org.')

header RCVD_IN_DNSWL_LOW        eval:check_rbl_sub('dnswl-firsttrusted',
'127.0.\d+.1')
describe RCVD_IN_DNSWL_LOW      Sender listed at http://www.dnswl.org/, low
trust
tflags RCVD_IN_DNSWL_LOW        nice net

header RCVD_IN_DNSWL_MED        eval:check_rbl_sub('dnswl-firsttrusted',
'127.0.\d+.2')
describe RCVD_IN_DNSWL_MED      Sender listed at http://www.dnswl.org/, medium
trust
tflags RCVD_IN_DNSWL_MED        nice net

header RCVD_IN_DNSWL_HI         eval:check_rbl_sub('dnswl-firsttrusted',
'127.0.\d+.3')
describe RCVD_IN_DNSWL_HI       Sender listed at http://www.dnswl.org/, high
trust
tflags RCVD_IN_DNSWL_HI         nice net

score RCVD_IN_DNSWL_LOW         -1
score RCVD_IN_DNSWL_MED         -10
score RCVD_IN_DNSWL_HI          -100
```

Другие правила в local.cf

- http://wiki.apache.org/spamassassin/WritingRules

Полный список наших правил (на 06.07.2011):

```
# Правило на рашу федерашу, фашисты взвинтили score в конфиге
# по-умолчанию до такой степени, что все наши письма для них
```

```
# теперь спам. Но это, к счастью, поправимо.
score FSL_RU_URL 0.0001 0.0001 -1.0 -1.0

auto_whitelist_path        /etc/mail/spamassassin/auto-wl/auto-whitelist
auto_whitelist_file_mode   0666

use_razor2              1
use_pyzor               1

# Our university
whitelist_from_rcvd *@rsu.edu.ru rsu.edu.ru
whitelist_from_rcvd *@rspu.ryazan.ru rsu.edu.ru
whitelist_from_rcvd *@ttc.ryazan.ru rsu.edu.ru
whitelist_from_rcvd *@www.rsu.edu.ru rsu.edu.ru
whitelist_from_rcvd *@proxy.rsu.edu.ru rsu.edu.ru

# whitelist subscribe.ru:
whitelist_from_rcvd *@subscribe.ru subscribe.ru

whitelist_from_rcvd *@sura.ru mail.sura.ru

# Удмуртский госуниверситет
whitelist_from_rcvd *@uni.udm.ru udsu.ru

# Рязанский радиотехнический
whitelist_from_rcvd *@rsreu.ru post.rsreu.ru

# Novell
whitelist_from_rcvd *@novell.com novell.com

# 163.com - китайский "Яндекс"
whitelist_from_rcvd *@163.com 163.com

whitelist_from_rcvd *@sfpgu.ru mail.sfpgu.ru

# ЦентрТрансТелеком
whitelist_from_rcvd *@centrettc.ru centrettc.ru

# МТТ
whitelist_from_rcvd *@mtt.ru mtt.ru

whitelist_from_rcvd *@unicreditgroup.ru unicreditgroup.ru

# N-Link
whitelist_from_rcvd *@nlink.ru nlink.ru

# АйПи-Тех
whitelist_from_rcvd *@iptechs.ru nlink.ru

# Системный интегратор Элетек
whitelist_from_rcvd *@eletek.ru eletek.ru

whitelist_from_rcvd *@mail.zakazrf.ru mail.zakazrf.ru

# Рязанская электросвязь
whitelist_from_rcvd *@mail.ryazan.ru mail.ryazan.ru

# Полярный институт
whitelist_from_rcvd *@pinro.ru pinro.ru
```

```
# Мейлрушечка
whitelist_from_rcvd *@mail.ru mail.ru
whitelist_from_rcvd *@list.ru mail.ru
whitelist_from_rcvd *@bk.ru mail.ru

# Яндекс
whitelist_from_rcvd *@yandex.ru yandex.ru
whitelist_from_rcvd *@narod.ru yandex.ru

# Гуголь
whitelist_from_rcvd *@gmail.com google.com

# Yahoo!
whitelist_from_rcvd *@yahoo.com yahoo.com

# SourceForge
whitelist_from_rcvd *@lists.sourceforge.net lists.sourceforge.net

# SunRav
whitelist_from_rcvd *@sunrav.ru kyoto.hostforweb.net

# Воронежская Государственная Технологическая Академия
whitelist_from_rcvd *@vgta.vrn.ru vgta.vrn.ru

# Живаго-банк
whitelist_from_rcvd *@zhivagobank.ru mail.zhivagobank.ru
whitelist_from_rcvd *@mail.zhivagobank.ru mail.zhivagobank.ru

# CGP Russial maillist
whitelist_from_rcvd *@mx.ru mx.demos.su

# В соотв-ии с РД №15-240 от 28.01.2011 Мин-ва обр-я РФ
# ------------------
# Адрес техподдержки системы ИАС "Мониторинг":
# support@is-mon.ru
# +7 (965) 226-28-53
# ------------------
whitelist_from_rcvd *@is-mon.ru mail.miigaik.ru

whitelist_from_rcvd *@forest.ru mail.forest.ru
whitelist_from_rcvd *@biodiversity.ru mail.biodiversity.ru

whitelist_from_rcvd *@assist.ru smtp.assist.ru

# Мегаплан
whitelist_from_rcvd *@megaplan.ru megamonstr.megaplan.ru

# Госзакупки
whitelist_from_rcvd *@zakupki.gov.ru zakupki.gov.ru

# Мегафон-Центр
whitelist_from_rcvd *@megafoncenter.ru mail.megafoncenter.ru

whitelist_from  *@rustest.ru

whitelist_from  *.neweurasia.ru
whitelist_from  *@neweurasia.ru
whitelist_from  *@mac.com
whitelist_from  *@staff.mesi.ru
whitelist_from  *@transtk.ru
```

```
whitelist_from  *@col.ru
whitelist_from  *@rsr-online.ru
whitelist_from  *@post.rzn.ru
whitelist_from  *.sovcombank.ru
whitelist_from  *@bti.secna.ru
whitelist_from  *@rcic.altai.ru
whitelist_from  *.nsu.ru
whitelist_from  *@sgu.ru
whitelist_from  *@dspl.ru
whitelist_from  *@csu.ru
whitelist_from  *@psu.ru
whitelist_from  *@vsu.by
whitelist_from  *@sgap.ru
whitelist_from  *.rsu.ru
whitelist_from  *@ministry.ru
whitelist_from  *.ministry.ru
whitelist_from  *.bsu.edu.ru
whitelist_from  *@bsu.edu.ru
whitelist_from  *.ibm.ru
whitelist_from  *.ibm.com
whitelist_from  *@teletesting.ru
whitelist_from  *.msu.ru
whitelist_from  *@msu.ru
whitelist_from  *@forum-media.ru

# Верим в веб-интерфейс Pronto!
header PRONTO X-Mailer =~ /CommuniGate\ Pro\ Pronto/
describe PRONTO Pronto msiler is good
score PRONTO -2.5

# Верим ребятам, сумевшим прописать у себя корректный SPF
header SPF_OK Received-SPF =~ /pass/
describe SPF_OK SPF test passed
score SPF_OK -1.0

# Гуголь
header GOOG Received =~ /.google.com/
describe GOOG google.com is good
score GOOG -4

# Яндекс
header YNDX Received =~ /.yandex.ru/
describe YNDX Yandex is good
score YNDX -4

header YNDX2 Received =~ /.yandex.net/
describe YNDX2 Yandex is good
score YNDX2 -4

# Укаинские мудаки
header ONLINE_UA Received =~ /mail.online.ua/
describe ONLINE_UA mail.online.ua is a SPAM relay
score ONLINE_UA 4

# Питерские мудаки
header INTERZET Received =~ /mail.interzet.ru/
describe INTERZET mail.interzet.ru is a SPAM relay
score INTERZET 4

# 99% спама и 1% уродских прог шлют почту без заголовка "To:" в header'ах
header HAVE_TO_HEADER exists:To
```

```
meta NO_TO_HEADER !HAVE_TO_HEADER
describe NO_TO_HEADER There is no To header
score NO_TO_HEADER 4

# Ужас под названием smtp[0-9]+.orange.fr, спама 90%, smtp-сервер
# для половины Франции.
header ORANGE_FR Received =~ /.orange.fr/
describe ORANGE_FR smtp.orange.fr is a SPAM relay
score ORANGE_FR 4

# This test works badly with cgpav, who cuts messages larger than 50K
score MIME_MISSING_BOUNDARY 0

# Cool rule, checking if both of sender & receiver of message are not in our
domain
header WOOD_FROM From =~ /rsu.edu.ru/i
header WOOD_TO1 To =~ /rsu.edu.ru/i
header WOOD_TO2 To =~ /rspu.ryazan.ru/i
header WOOD_TO3 To =~ /ttc.ryazan.ru/i
#meta WITHOUT_OUR_DOMAIN !WOOD_FROM && (!WOOD_TO1 || !WOOD_TO2 || !WOOD_TO3)
meta WITHOUT_OUR_DOMAIN !WOOD_FROM && !(WOOD_TO1 || WOOD_TO2 || WOOD_TO3)
describe WITHOUT_OUR_DOMAIN Sender and receiver are not in our domain
score WITHOUT_OUR_DOMAIN 2.5

# CGP blacklist-admin@ ruleset - dozen of spammers use this address to spam
header LOCAL_TO_BA To =~ /blacklist-admin\@cgp\.rsu\.edu\.ru/i
describe LOCAL_TO_BA Mail to blacklist-admin@, probably SPAM
score LOCAL_TO_BA 4.5

# Rulestet for checking reverse connection feature of CGP
# ------------------------------------------------------------
header REV_CHECK_DROPPED X-Reverse-Check =~ /connection closed by peer/
describe REV_CHECK_DROPPED Reverse check connection of sender mail address
closed by remote server
score REV_CHECK_DROPPED 4

header REV_CHECK_FAILED X-Reverse-Check =~ /address rejected with reverse-
check/
describe REV_CHECK_FAILED Reverse check of sender mail address rejected by
remote server
score REV_CHECK_FAILED 4.5

header REV_CHECK_NORELAY X-Reverse-Check =~ /no relay available/
describe REV_CHECK_NORELAY No relay available for reverse check
score REV_CHECK_NORELAY 4.5

header REV_CHECK_NORESP X-Reverse-Check =~ /no response/
describe REV_CHECK_NORESP No response from remote server to reverse check of
sender mail address
score REV_CHECK_NORESP 4

header REV_CHECK_PROTOERR X-Reverse-Check =~ /reverse check protocol error/
describe REV_CHECK_PROTOERR Reverse check protocol error on remote server
score REV_CHECK_PROTOERR 4

header REV_CHECK_REFUSED X-Reverse-Check =~ /connection refused/
describe REV_CHECK_REFUSED Reverse check of sender mail address refused by
remote server
score REV_CHECK_REFUSED 4.5

header REV_CHECK_TIMEOUT X-Reverse-Check =~ /read time-out/
describe REV_CHECK_TIMEOUT Reverse check of sender mail address timed out
```

```
score REV_CHECK_TIMEOUT 4

# DNSBL
# ------------------------------------------------------------------
# URL: http://www.barracudacentral.org/rbl/
header __RCVD_IN_BRBL eval:check_rbl('brbl', 'b.barracudacentral.org')
describe __RCVD_IN_BRBL received via a relay in b.barracudacentral.org
header RCVD_IN_BRBL_RELAY eval:check_rbl_sub('brbl', '127.0.0.2')
tflags RCVD_IN_BRBL_RELAY net
describe RCVD_IN_BRBL_RELAY received via a relay rated as poor by Barracuda
score RCVD_IN_BRBL_RELAY 3.00
```

Проверка наличия ошибок в правилах:

```
spamassassin --lint
```

Кнопки спам/не спам в веб-интерфейсе CGP

Скачиваем скрипты с сервера Stalker: ftp://ftp.stalker.com/pub/stuff/noarch/SpamPackage-scripts.tar.gz и устанавливаем по инструкции.

В административном веб-интерфейсе идем Пользователи -> Центральный Справочник, находим "Дополнительные Установки Пользователя" и в группу "Системные" добавляем 2 занчения:

```
SpamFilterEnabled
SpamFilterLevel
```

Редактируем скрипты из пакета SpamPackage, устанавливаем корректный пароль Postmater'a и редактируем название папки для спама, а так же меняем адерса для жалоб на локальные ящики SpamAssassin

Дальше, создаем папку и устанавливаем права:

```
mkdir /var/CommuniGate/CGI
chown root:mail /var/CommuniGate/CGI
```

Копируем в нее указанные скрипты с правами 0755

В административном веб-интерфейсе идем Установки -> Услуги -> HTTPU и добавляем в раздел "CGI Программы":

- CGI Каталог: /var/CommuniGate/CGI
- Расширение имени файла: pl
- Программа-Интерпретатор: /usr/bin/perl -w

В папке /opt/CommuniGate/WebSkins/Simplex находим файл strings.data и меняем следующие параметры:

- prefJunkMailboxName = "SPAM";
- SpamPackageEnabled = "Yes";
- SpamRecipient = "learn-spam@имя-домена";
- NotSpamRecipient = "learn-ham@имя-домена";

Q: Подскажите, как правильно менять настройки в strings.data? Если загрузить изменённый файл в скин, то язык веб-интерфейса переключается на английский и сменить его нельзя. При редактировании самого файла скина (/opt/CommuniGate/WebSkins/strings.data) этого не происходит, но он перезаписывается при каждом обновлении CGP, что тоже не очень удобно.

A: В исправленном strings.data должны быть только исправленны строки и словари. То, что не менялось, в кастомный strings.data писать не надо.

Поддержка DKIM / DomainKeys

Можно поставить бесплатный perl-скрипт, который работает через Content-Filtering [16] [17]. Вручную потребуется поставить перл модули*Mail::DKIM*, и указать путь к приватному ключу для домена.

```
#!/bin/perl
#
# DKIM/DomainKeys signer for CommuniGate CGP free (implemented as a Content-
Filtering script)
#
# Copyright (c) 2005-2007 Valera V.Kharseko. This program is free software.
```

```
# You can redistribute it and/or modify it under the terms of the
# GNU Public License as found at http://www.fsf.org/copyleft/gpl.html.
#
# Written by vharseko@xxlive.ru.

use Mail::DKIM::Signer;
use Mail::DKIM::DkSignature;
use Mail::DKIM::TextWrap;


use Getopt::Long;
use Pod::Usage;

my $CustomHeader = "X-DKIM-Signed:"." yes";

sub signer_policy {

    my $dkim = shift;
    $dkim->add_signature(Mail::DKIM::DkSignature->new(
        Algorithm => "rsa-sha1",
        Method    => "simple",
        Headers   => $dkim->headers,
        Domain    => $dkim->message_sender->host,
        Selector  => "default",
        Expiration => time() + 86400,
        Identity   => $dkim->message_sender->address
    ));

    $dkim->add_signature(Mail::DKIM::Signature->new(
        Algorithm => "rsa-sha1",
        Method    => "relaxed",
        Headers   => $dkim->headers,
        Domain    => $dkim->message_sender->host,
        Selector  => "default",
        Expiration => time() + 86400,
        Identity   => $dkim->message_sender->address
    ));
    return;


}

sub Log {

        print "* $_[0]\n";
}
$| = 1;
Log "DKIM is running";Log "";
mkdir "Submitted" if ( !-d "Submitted" ); while (<>) {

    my @line = split( / /, $_ );
    chomp( $line[0] );
    print "$line[0] OK\n"     and next if ( $line[1] =~ /^quit$/i );
    print "$line[0] INTF 3\n" and next if ( $line[1] =~ /^intf$/i );
    print "$line[0] OK\n"     and next if ( $line[1] =~ /^key$/i );
    print "$line[0] FAILURE\n" and next if ( $line[1] !~ /^file$/i );
    $line[2] =~ s|\\|/|g;
    chomp( $line[2] );

    Log "DKIM process: $line[2]";

    if ( !open( MSG, $line[2] ) ) {
```

```
        Log "Error: file not found $line[2]";
        print "$line[0] OK\n";
    }
    else {
        my ( $sender, @recipients );
        #CGP headers
        while (1) {
            $line = <MSG>;
            chomp($line);
            last if ( $line eq '');
            if ( $line =~ /^(\w).+<(.+)>/ ) {
                if ( $1 eq 'P' ) {
                    $sender = $2;
                }
                else {
                    push @recipients, $2;
                }
            }
        }
        #mail headers and body
        my $EntireMessage="";
        my $dkim = new Mail::DKIM::Signer(Policy => \&signer_policy,KeyFile =>
"d:/CommuniGate/rsa.private");
        while (<MSG>){
            $EntireMessage=$EntireMessage.$_;
            chomp $_;
            s/\015?$/\015\012/s;
            $dkim->PRINT($_);
        }
        close MSG;

        if ( $EntireMessage !~ /$CustomHeader/i ) {
            $dkim->CLOSE;
            Log "DKIM sign for user=".($dkim->message_sender->address)."
domain=".($dkim->message_sender->host);

            my $signature_dk=($dkim->signatures())[0]->as_string;
            $signature_dk=~s/\s//g;
            Log "$signature_dk";

            my $signature_dkim=($dkim->signatures())[1]->as_string;
            $signature_dkim=~s/\s//g;
            Log "$signature_dkim";

            my $alertFileName.="Submitted/A".time().int(rand(10000));
            open(SUBM,">$alertFileName.tmp");
            print SUBM "$CustomHeader\n";
            print SUBM "$signature_dk\n";
            print SUBM "$signature_dkim\n";
            print SUBM $EntireMessage;
            close SUBM;
            rename("$alertFileName.tmp","$alertFileName.sub");
            print "$line[0] DISCARD\n";
        }
        else {
            Log "DKIM skip file: $line[2]";    print "$line[0] OK\n";
        }
    }
    open STDOUT, ">&STDOUT";


}
```

LDAP

Аутентификация пользователей на прокси-сервере Squid

Communigate можно использовать в связке с proxy-сервером squid

В настойках communigate:

Включаем **Управление Пользователями через LDAP**:

Пользователи -> Центральный справочник

Управление Пользователями через LDAP: Включено

Проверка:

```
squid_ldap_auth -b "cn=domain.name" cgp-server.com
```

Должно выдавать OK/ERR на plaintext-строку "имя пароль"

В конфигурационном файле squid.conf:

```
# (CommuniGate LDAP)
auth_param basic program /usr/sbin/squid_ldap_auth -b "cn=example.com"
cgp.example.com
auth_param basic children 10
auth_param basic realm RSU proxy-server
auth_param basic credentialsttl 2 minutes
```

(Подробнее: Настройка_SQUID#CommuniGate_Pro)

Firewall

На хосте (SLES) в файле */etc/sysconfig/SuSEfirewall2* добавляем следующие строки:

```
FW_SERVICES_EXT_TCP="21 25 53 80 110 143 387 443 465 587 636 674 993 995
1024:65535"
FW_SERVICES_EXT_UDP="53 69 1024:65535"
```

Для того, чтобы защитить хост от брута по ssh в этом же файле делаем следующие изменения:

```
FW_SERVICES_ACCEPT_EXT="0.0.0.0/0,tcp,
22,,hitcount=3,blockseconds=60,recentname=ssh"
```

На роутере (SLES) для белой сети для каждого из ip-адресов, назначенных серверу:

/etc/sysconfig/SuSEfirewall2

```
FW_FORWARD="0/0,91.203.180.144/28,tcp,25 \
            0/0,91.203.180.144/28,tcp,80 \
            0/0,91.203.180.144/28,tcp,119 \
            0/0,91.203.180.144/28,tcp,443 \
            0/0,91.203.180.144/28,tcp,465 \
            0/0,91.203.180.144/28,tcp,587 \
            0/0,91.203.180.144/28,tcp,993 \
            0/0,91.203.180.144/28,tcp,3478 \
            0/0,91.203.180.144/28,udp,3478 \
            0/0,91.203.180.144/28,tcp,3479 \
            0/0,91.203.180.144/28,udp,3479 \
            0/0,91.203.180.144/28,tcp,5060 \
            0/0,91.203.180.144/28,udp,5060 \
            0/0,91.203.180.144/28,tcp,5061 \
            0/0,91.203.180.144/28,udp,5061 \
            0/0,91.203.180.144/28,tcp,5222 \
            0/0,91.203.180.144/28,udp,5222 \
            0/0,91.203.180.144/28,tcp,5223 \
            0/0,91.203.180.144/28,udp,5223 \
            0/0,91.203.180.144/28,tcp,5269 \
            0/0,91.203.180.144/28,udp,5269 \
            0/0,91.203.180.144/28,tcp,11024:11025 \
            0/0,91.203.180.144/28,tcp,60000:60099 \
            0/0,91.203.180.144/28,udp,60000:60999 \
```

Подробнее о портах:

- 25 и 587 - SMTP
- 993 - IMAP (ssl)
- 80 и 443 - веб-интерфейс пользователя http, https
- 3478 и 3479 - STUN
- 5060, 5061 - SIP
- 5222, 5223, 5269 - Jabber/XMPP
- 11024:11025 и 60000:60999 - голосовой трафик RTP

Коммуникации реального времени

Медиа плагин для браузеров Internet Explorer, Firefox, Chrome и Safari доступен по адресу: http://www.communigate.com/MediaPlugin/

Настройка SIP-шлюза

Исходящие вызовы

Если вы предполагаете использовать одну учетную запись (SIP ID) для всех аккаунтов в различных доменах:

```
Users -> Account Defaults -> PSTN
Gateway Domain: sip-provider.example.com
Gateway Address:
Caller ID: SIP_ID или *
Name for Gateway: SIP_ID@sip-provider.example.com
```

Если нет, необходимо произвести настройки PSTN для каждого домена:

```
Users -> Domains -> ваш_домен -> Account Defaults -> PSTN
```

или пользователя:

```
Users -> Domains -> ваш_домен -> Objects -> ваш_акаунт -> Real-Time -> PSTN
```

Входящие вызовы

Настроить входящие вызовы, вы можете настроив регистрацию средствами CommuniGate Pro:

(для версий ниже чем 5.3.c3)

```
Settings -> Real-Time -> SIP -> Gateways ->
GatewayName: sip-provider                Authenticate: Disabled
Domain: sip-provider.example.com         Proxy: None
Username: SIP ID                         Contact: pbx@ваш_домен
AUTH name:                               Register Every: 2 min
Password: пароль
```

RSIP - доступен начиная с релиза 5.3c3

```
Setting -> Users -> главный домен (main domain) -> аккаунт pbx -> Real Time ->
RSIP
```

Далее, загружаем файлы для поддержки русского языка PBX [2] (в архиве находятся russian_female.tar и russian_sppi.tar)

```
Users -> Domains -> ваш_домен -> PBX -> Create Custom Environment
Languages -> Create -> Russian
Переходим в Languages -> Russian, Upload File -> загружаем последовательно
russian_female.tar и russian_sppi.tar
```

Затем настраиваем Авто-секретарь:
Users -> Domains -> ваш_домен -> Objects -> выбираем аккаунт pbx -> Real-Time -> Advanced -> Auto-Attendant
Language Menu: Custom: Russian (English,при необходимости)
Department Menu:Custom: можно удалить sales, techsupport, conference, operator

(если у вас нет соответсвующих отделов и вам не нужна конференция)
Directory Prefix: Custom: X <--- первая цифра алиасов (псевдонимов) ваших пользователей
Directory Digits: Custom: X <--- количество цифр в псевдонимах
Жмем Update.

Для звонков через Sipbroker добавьте следующую строку в Router
N:S:<**@*> = **@sipbroker.com

- http://wiki.sipnet.ru/index.php/Категория:CommuniGatePro
- http://mx.demos.su/lists/cgp-russian/2010_06/16520.html

Хитрости Маршрутизатора

Выделяем целый домен под spamtrap's:

```
M:<*@example.com> = spamtrap
```

Маршрутизация телефонии:

```
<911@*>       = emergency@localhost  ; 911: NA emergency
<112@*>       = emergency@localhost  ; 112: EU emergency
<01@*>        = emergency@localhost  ; 01:  RU emergency
S:<emergency> = emergency#pbx        ; start 'emergency' app
<7(2d)@*>     = pbx{*}#pbx           ; 7nn calls go to PBX

<(4d)@*> = *@telnum ; пусть нумерация 4-значными будет сквозной
<(6d)@*> = +74912*@telnum ; костылик для 6-значных
<(10d)@*> = +7*@telnum ; считаем 10-значные российскими
<+(5-15d)@*> = +*@telnum

<+(d)@*> = +*@telnum ; прямой +номер в e164 домен "telnum"
<8(10d)@*> = +7*@telnum ; костыль для звонящих через 8-ку
telnum = e164.arpa.enum ; прямой +номер в e164.arpa
S:e164.arpa.noenum = pstn

S:<+7(10d)@pstn> = gatewaycaller{8*,nlink}#postmaster@localhost
S:<8(10d)@pstn> = gatewaycaller{8*,nlink}#postmaster@localhost
S:<(5-15d)@pstn> = gatewaycaller{*,nlink}#postmaster@localhost

S:<(4d)@pstn> = pbx#pbx@localhost
```

Входящие телефонные звонки

- https://support.communigate.com/tickets/kb_article.php?ref=1559-WEIA-9110

E.164

https://mail.istu.ru/Guide/russian/Router.html#ENUM

Подключаем ENUM-домены:

- e164.arpa
- e164.org
- e164.info
- enum.org

Правим маршрутизатор:

```
<+(d)@*> = +*@telnum ; прямой +номер в e164 домен "telnum"
<8(10d)@*> = +7*@telnum ; костыль для звонящих через 8-ку
telnum = e164.arpa.enum ; прямой +номер в e164.arpa
S:e164.arpa.noenum = pstn
```

Проверить работоспособность номеров в E.164 можно при помощи сервиса http://enumquery.com/

Входящие звонки

В Маршрутизаторе укажем, что входящий звонок с многоканального номера перенаправляем на PBX нужного

домена:

```
<out_login_at_ext_service@main_domain_ip> =  pbx{*}#pbx@example.com
```

Создаем в интересующем нас домене пользователя **pbx** с псевдонимами 200 и conference. Даем ему права доступа:

- Может менять установки Этого Домена и его Пользователей
- Полный доступ ко всем Файлам
- Может выступать от имени других

Во вкладке **Real-Time** добавляем правило **PBX Center starter** со следующим содержимым:

```
Данные ---
Равно:
Действие: Перенаправить к
Параметр: #pbx
```

Во вкладке **Прочее** выбираем параметры **Directory Prefix** равным числу, с которого начинаются внутренние тлф. номера пользователй и**Directory Digits** равным общему числу цифр во внутреннем номере.

- http://mail.stalker.com/Guide/russian/PBXCenter.html#AutoAttendant

Программирование PBX-приложений на CG/PL:

- http://freewind.habrahabr.ru/blog/89142/

Перенаправление звонков

Q: Каким образом нужно создать правило при входящем вызове абонента, при условии, что вызываемый абонент занят (486) и его нужно перенаправить на другого абонента?

A: Создайте правило без условий с одним действием - Fork или Redirect на нужный номер. А потом для созданного правила выберите stage == busy.

Перехват звонков

Q: Возможно ли "перехватить" звонок? То есть у коллеги звонит трубка, а я не вставая со своего места набираю что-нибудь со своей и получаю звонок себе.

A: Да, можно. В таблице "Маршрутизатор" по умолчанию есть запись:

```
<8(3d)@*> = pickup{*}#pbx
```

Ещё у вас должны быть административные права видеть все звонки, либо пользователь должен дать вам право видеть его звонки явно (WebUser -> Folders -> Management -> Account Rights -> Call Control)

Перехват осуществляется звонком на 8XXX, где XXX - номер "экстеншена", который звонит.

QoS

Procurve 5304xl

Для SIP-трафика в консоли свитча:

```
conf
qos tcp-port 5060 priority 6
qos udp-port 5060 priority 6
```

Проверка:

```
sh qos tcp-udp-port-priority
```

Выбираем VLAN для голосового трафика и поднимаем ему приоритет:

```
conf
vlan XX
qos priority 6
```

Проверка:

```
sh qos vlan-priority
```

Записываем изменения во flash-память:

```
write mem
```

SIP/Jabber

DNS записи являются типичным источником ошибок конфигурации SIP и XMPP.

Так же, как записи e-mail и MX, они представляют собой особый тип DNS-записей для маршрутизации и приоритезации SIP и XMPP. Такие записи называются служебными или "SRV" записями.

Используя утилиты DNS-резолвинга, такие как "dig", "nslookup", и д.р. можно запросить эти записи для лучшего понимания маршрутизации SIP и XMPP. Синтаксис сначала может показаться немного чудным, так как он использует application protocol (_sip) и IP protocol (_udp) компоненты:

Code:

```
$ dig SRV _sip._udp.versature.com


;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31515
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 9, ADDITIONAL: 10

;; QUESTION SECTION:
;_sip._udp.versature.com. IN SRV

;; ANSWER SECTION:
_sip._udp.versature.com. 6611 IN SRV 10 0 5060 login.versature.com.
```

Нужно отметить, что в данном примере ответ содержет (по крайней мере) три важные информационные части: 10 - приоритет сервера по сравнению с возможными другими серверами для той же записи 5060 - порт к которому осуществляется подключение

login.versature.com - имя сервера

Также возможны множественные записи:

Code:

```
$ dig SRV _sip._udp.communigate.com


;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40722
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 7

;; QUESTION SECTION:
;_sip._udp.communigate.com. IN SRV

;; ANSWER SECTION:
_sip._udp.communigate.com. 3600 IN SRV 0 0 5060 post.communigate.com.
_sip._udp.communigate.com. 3600 IN SRV 1 0 5060 site.communigate.com.
```

В данном примере сервер "post.communigate.com" имеет приоритет "0" и поэтому он выше, чем у сервера site.communigate.com.

SIP UDP клиенты должны попытаться соединиться сначала с post.communigate.com, а лишь потом с site.communigate.com.

Далее следует пример полной DNS-записи для SIP и XMPP для вымышленного домена "example.com", использую синаксис BIND:

Code:

```
example.com IN SOA ns.example.com. postmaster.example.com. (
2007042300 ; Serial
36000 ; Refresh
9000 ; Retry
3600000 ; Expire
36000) ; Minimum
```

```
; SIP
_sip._udp 3600 IN SRV 10 0 5060 mail.example.com.
_sip._tcp 3600 IN SRV 10 0 5060 mail.example.com.
_sips._tcp 3600 IN SRV 10 0 5061 mail.example.com.
_sips._udp 3600 IN SRV 10 0 5061 mail.example.com.
; XMPP
_xmpp-server._tcp 3600 IN SRV 10 0 5269 mail.example.com.
_xmpp-server._udp 3600 IN SRV 10 0 5269 mail.example.com.
_xmpp-client._tcp 3600 IN SRV 10 0 5222 mail.example.com.
_xmpp-client._udp 3600 IN SRV 10 0 5222 mail.example.com.
_jabber._tcp 3600 IN SRV 10 0 5269 mail.example.com.
_jabber._udp 3600 IN SRV 10 0 5269 mail.example.com.
_jabber-client._tcp 3600 IN SRV 10 0 5222 mail.example.com.
_jabber-client._udp 3600 IN SRV 10 0 5222 mail.example.com.
```

Онлайн-генератор SRV записей:

- http://www.jms1.net/jabberd2/srv.shtml

Онлайн проверка SRV записей:

- http://kingant.net/check_xmpp_dns/

IP-телефоны

Основная статья: Настройка IP-телефонов

Софтофоны

Основная статья: IP-телефон на ПК (Софтофон)

Софтофон веб-клиента Pronto!

> **Это незавершённая статья, требующая доработки.**
> Описать как пользоваться, как ставить media plugin, какие порты д.б. открыты на брандмауере.

Apple iChat

Реализация для обычного 3rd-party клиента (iChat) на сервере очень проста.

1. Включите приемники XMPP на CGP сервере
    1. Settings->RealTime-> XMPP->Recieving->Listener
    2. Откройте порты 5222 (SSL off), 5223 (SSL on), 5269 (SSL off).
2. Проверьте, что приемник CGP работает. В *nix и Mac используйте "netstat -lnp | grep 522" и проверьте, что CGServer ожидает соединения.
3. Проверьте, включен ли XMPP для доменных пользователей.
    1. Выберите аккаунт пользователя в интерфейсе администратора. Убедитесь, что в Enabled Services есть запись: +XMPP. Если же теё нет, включите её, выбрав Domain Settings и включив её (для всех доменов сервера)
4. Открыть порты на фаерволе (сервер и сеть)
    1. TCP для всех указанных выше портов.
5. Настройте клиент для подключения к серверу.
6. Следуйте инструкциям "iChat as your IM client" на http://www.communigate.com/main/tips/

Troubleshooting SIP

How do I investigate or troubleshoot a SIP-related problem? [18]

Troubleshooting SIP can be a detailed effort, because of integration issues and ever-evolving standards within the SIP industry. However, CommuniGate Pro provides good ways to investigate these problems:

SIP Log Levels

Please be sure your CommuniGate Pro system/cluster is logging all SIP related modules at log level "All Info", and please provide the logs on this call, for debugging purposes.

Please increase your log levels to "All Info" in these areas of the WebAdmin Interface:

```
Settings->Real-Time->Signals
Settings->Real-Time->Nodes
Settings->Real-Time->SIP->Sending
Settings->Real-Time->SIP->Receiving
```

Perform a test call, then grab the logs.

Media-related Log Levels

CommuniGate Pro can function both as a media proxy and a media termination (PBX, voicemail) system. This includes both "Class 4" and "Class 5" features.

In order to gather debugging information for media, there are two locations within the WebAdmin Interface where you can log the media traffic at "All Info":

```
Media Proxy Log Levels: Settings->Network->LAN IPs: Media Proxy
Media Termination & Nodes: Settings->Real-Time->Media
```

Log Investigation

There is a built-in method for grabbing detailed related logs in CommuniGate Pro. If you go to *Monitors->Logs*, first find the first "REGISTER" or "INVITE" portion of the attempt. In that transaction, you will find a Call-ID. If you copy the Call-ID, then paste it into "Filter", you can do a "Keyed" log query.

For example, find the Call-ID:

```
Call-ID: MWVjYTIzNmFhZGEyNjc3ZTczNzY5MzNkMTE5ZjczMmQ.
```

Paste this into "Filter", select "Keyed", then hit "Display". The logs will then be displayed for the entire SIP conversation. If using a SIP Farm/Dynamic Cluster, you may need to perform this log gathering on each Frontend node in the Cluster.

WebAdmin Monitors

The monitoring pages at *Monitors->Real-Time* provide good real-time information about SIP transactions. For example, all active/failed registrations to PSTN gateways should be available at *Monitors->Real-Time->Nodes*.

WebAdmin/SNMP data

The "Statistics" pages in CommuniGate Pro WebAdmin provides insight into ongoing performance. These Statistics are also available through the SNMP interface to CommuniGate Pro. *Monitors->Statistics*

The following Statistics are particularly useful for debugging VoIP issues:

```
sipTCPConnectionsActive
sipTCPConnectionsTotal
sipEnqueuedPackets
sipServersActive
sipServersTotal
sipClientsActive
sipClientsTotal
proxyActive
signalActive
signalTotal
realTimeNodeActiveEvents
realTimeNodeTotalThreads
```

ТЕСТИРОВАНИЕ

Способности SpamAssasin распознавать спам

```
spamassassin -t < sample-spam.txt > /tmp/sample-spam.txt
spamassassin -t < sample-nonspam.txt > /tmp/sample-nonspam.txt
```

Работа clamav через cgpav

Скопируйте тестовый вирус eicar.com в директорию */var/CommuniGate* и запустите cgpav:

```
cd /var/Communigate
wget "http://www.eicar.org/download/eicar.com"
./cgpav
```

Появится консоль ввода фильтра.

Введите:

```
1 FILE eicar.com
```

cgpav работает нормально если вы видите

```
1 ERROR "WARNING! Your message was infected by VIRUS: EICAR-AV-Test"
```

Или же, программа может по каким-то причинам не найти вирусов

```
1 OK
1 REJECTED "Antiviral filter unavailable. Will try later"
```

Программирование

Communigate PBX[19], CG/PL[20]

Воспроизвести сообщение группе пользователей

Пользователь: alert, номер 2431 Пользователи > домен example.com > пользователь alert Real-Time > Установки Звонков > Телефонные Номера добавьте 2431 Real-Time > Правила для входящих звонков добавьте новое правило:

```
Данные: ---
Операция: равно
Параметр:
Действие: Перенаправить к #example-signal
```

- Группа: group-example создайте в домене example.com и добавьте в нее пользователей с доб. номерами и переадресацией или ip-аппаратами, моб. и гор. телефоны
- Аудиофайл: запишите сообщение (в Audacity сохраните как 16 bit PCM .wav) message.wav и загрузите на закладке PBX домена example.com

Скрипт будет обзванивать пользователей и номера телефонов из группы group-example и проигрывать сообщение message.wav

example-signal.sppr (загрузите на закладке PBX домена example.com):

```
//
// Sample: StartBridge()/AcceptBridge()/BreakBridge()
//   Accept an incoming call (stop if it's not possible).
//   Create a new Task to run the Caller code,
//     and send it an Event with the URI to dial.
//   Play the PleaseWait media file.
//   Wait for a StartBridge Event from the Caller Task.
//   Accept it and loop till the user disconnects.
//
//   The Caller code:
//   Receive a URI to call as an Event from the parent Task
//   Connect to the URI and play the YouGotACall media file
//   StartBridge with the parent, loop till the user disconnects
//
function authenticatedSelfCall2(userName) external;
entry Caller forward;
procedure ControlBridge() forward;

entry Main is
```

```
      if AcceptCall() != null then stop; end if;
      SysLog("ACHTUNG(); AcceptCall()");
      address = "alert";
      if authenticatedSelfCall2(address) then
            accounts = ReadGroupMembers("group-example");
            if accounts == null then
                  stop;
            end if;

            account = "";
            myCount = 0;
            myLength = length(accounts);
            while myCount < myLength loop
                  account = "sip:"+accounts[myCount]+"@"+MyDomain();
                  callerTask = spawn Caller;
                  if callerTask == null or else
                        SendEvent(callerTask,"dial",account) != null then
                              PlayFile("Failure");
                        stop;
                  end if;
                  myCount = myCount + 1;
            end loop;
            PlayFile("thankyouforwaiting");
            void(BreakBridge());
      else
            PlayFile("Failure");
      end if;

      SysLog("ACHTUNG(); end entry");
end entry;

//
// Caller Task code
//
entry Caller is
      // wait for a "dial" event from the main task
      input = ReadInput(30);
      if input == null or input.what != "dial" then stop; end if;

      mainTask = input.sender;
      accountForDial = input.parameter;

      // Calling the URI specified as the Event parameter
      // If connection failed, send an Event back to the
      //  main task and quit
      //resultCode = StartCall(startEvent.parameter);
      resultCode = StartCall(input.parameter);
      if resultCode != null then
            void(SendEvent(mainTask,"result",resultCode));
            stop;
      end if;
      SysLog("ACHTUNG(); StartCall("+accountForDial+");");

      // wait for any Event other than provisional ones
      loop
            input = ReadInput(3600);
      exitif not IsCallProvisionEvent(input);
      end loop;

      // the parent has sent us "stop" - then we'll die immediately
      if IsDictionary(input) and then input.what == "stop" then stop; end if;
```

```
      if not IsCallCompletedEvent(input) or else input.parameter != null then
            void(SendEvent(mainTask,"result","generic error"));
            stop;
      else
            PlayFile("message16bitpcm.wav", 8000);
            SysLog("ACHTUNG(); PlayFile(): "+accountForDial);
      end if;

      // we have established a bridge
      //ControlBridge();
      void(BreakBridge());
      PlayFile("GoodBye");
end entry;

//
// Controlling the peer signaling:
// while the media is bridged:
//    exit if the peer hangs up, dials "#"
//  or if the bridge is removed
//
procedure ControlBridge() is
      loop
            input = ReadInput(3600);
      exitif IsBreakBridgeEvent(input) or else
                  IsDisconnectEvent(input) or else input == "#";
      end loop;
      void(BreakBridge());
end procedure;
```

authenticatedSelfCall2.sppi:

```
// ============================================== //
//      "External" login into own account         //
//                                                 //
// Version 1.2                                     //
// Copyright (c) 2005-2008, Stalker Software, Inc. //
// ============================================== //
procedure serviceDispatcher(command) external;
function readPIN(maxDigits) external;

function authenticatedSelfCall2(userName) is
  accountName = RouteLocalURI("sip:" + userName + "@" + MyDomain());
  if accountName == null then return false; end if;
  preferences = GetAccountPreferences("~" + accountName + "/" );
  if not IsDictionary(preferences) then return false; end if;
    PlayFile("EnterPIN"); PlayFile("FinishByPound");
    input = readPIN(20);
    if input == preferences.("AccessPIN") then
      ClearDTMF(); input = ReadInput(3); // just to wait for 3 seconds
        SysLog("ACHTUNG(); correct pin;");
        return true;
    end if;
  SysLog("ACHTUNG(); incorrect pin;");
  return false;
end function;
```

Минусы: Ложное срабатывание (PlayFile в логе)

- IP-аппарат, на котором есть ignore/dnd
- Мобильный, на котором настроена голосовая почта
- Аккаунты, на которых настроена голосовая почта, переадресация, а мобильный недоступен.

Отказоустойчивость

В целях надежного прохождения почты и уменьшения перебоев, связанных с авариями на каналах связи, почтовый сервер подключен к двум независимым провайдерам и имеет 2 белых ip-адреса. В DNS внесены оба адреса в качестве mx-записей домена.

Насторойка ОС

Порядок действий для SLES 9 SP3:

Добавляем 2 строчки в файл **/etc/iproute2/rt_tables**

```
9       viainet1
10      viainet2
```

Создаем в **/etc/sysconfig/network** каталог **iproute2**, в него кладем файл **iproute2_custom** (chmod +x):

```
#!/bin/bash

IP2=xxx.xxx.xxx.xxx       # ip от провайдера 1
IP3=yyy.yyy.yyy.yyy       # ip от провайдера 2

P1=iii.iii.iii.iii        # дефолтный шлюз
P2=jjj.jjj.jjj.jjj        # шлюз провайдера 1
P3=kkk.kkk.kkk.kkk        # шлюз провайдера 2

ip route replace default via $P2 table viaesv
ip route replace default via $P3 table viacttc

ip rule add from $IP2 table viainet1
ip rule add from $IP3 table viainet2

#ну и дефолтный маршрут:
ip route add default via $P1
```

Делаем символическую ссылку на этот файл в каталоге **/etc/sysconfig/network/if-up.d**:

```
ln -s /etc/sysconfig/network/iproute2/iproute2_custom /etc/sysconfig/network/
if-up.d/iproute2_custom
```

Теперь машина отвечает на пинги по на оба внешних ip.

АДМИНИСТРИРОВАНИЕ

Приветственное письмо новым пользователям системы

Идем в *Пользователи -> Домены -> (домен) -> Объекты -> Шаблон* и по инструкции создаем шаблон письма для пользователей, чтобы они помнили о нашей заботе и опеке.

Следует помнить, что напрямую русские символы в заголовках письма использовать нельзя.

> **Это незавершённая статья, требующая доработки.**
> Описать способ получения легитимного заголовка письма с русскими буквами: perl-скрипт или генерация почтовым клиентом.

Миграция пользователей со старой платформы

Старая почтовая система авторов построена на базе Postfix+Courier-IMAP с доступом пользователей через pop/smtp/imap и web-интерфейс squirrelmail. Информация о пользователях хранится в БД MySQL.

Процесс миграции включает в себя:

- Экспорт информации о аккаунтах старой системы в текстовый файл
- Создание аккаунтов пользоватей по шаблону на новой системе
- Миграция дерева папок IMAP и почтовых сообщений со старого сервера на новый
- Изменение dns-зон

Итак, приступим:

Экспорт информации о аккаунтах старой системы в текстовый файл

Формат импорта/экспорта communigate предполагает поля, разделенные знаком табуляции. В первой строчке указываются наименования полей.

Скрипт:

```
#!/bin/bash

MHOST="127.0.0.1"
LOGIN="sqllogin"
PASS="sqlpass"

QUERY=" SELECT login, name, password
        FROM users;"

mysql -h $MHOST --execute="$QUERY" --database="dbname" --user="$LOGIN" --
password="$PASS" | \
awk -F "|" \
'BEGIN { \
    print "Name" "\t" "RealName" "\t" "Password" \
} { printf("%s\t%s\t%s\n",$1,$2,$3);  }' | iconv -f koi8-r -t utf-8 >
account_list.txt
```

Создание аккаунтов пользователей по шаблону на новой системе

В административном интерфейсе communigate:

Пользователи -> Домены -> Имя_домена -> Объекты

Выбираем "Импортировать" указав путь к файлу

Миграция дерева папок IMAP и почтовых сообщений со старого сервера на новый

Communigate предоставляет утилиты для миграции. Они находятся в каталоге /opt/CommuniGate/Migration:

Команда:

```
./MoveAccounts --IMAP account_list.txt old_imap_ip communigate_domain_ip
```

Через некоторое время вся информация пользователей будет перенесена.

В случае, если миграция происходит из CGP в CGP, вполне можно обойтись простым копированием каталогов с аккаунтами и настройками. Для того, чтобы заполнился "Центральный справочник", необходимо в настройках домена в разделе Directory Integration нажать сначала Delete All, потом Insert All.

Модификация интерфейса Pronto!

Можно при необходимости заменить логотипы Communigate на свои собственные загрузив в папку со скином Pronto следующие файлы [3]:

- **loginlogoimage.png**

Главный логотип на странице входа. Размер: 350x117 пикселей, фон: прозрачный.

- **loginimage.png**

"screenshot image" на странице входа. Размер 440x340 пикселей, фон: непрозрачный.

- **logosmallimage.png**

Логотип в левом верхнем углу на странице входа. Размер: 90x30 пикселей, фон: прозрачный.

- **customlogosmall.png**

Логотип CommuniGate Pro с обрамлением в правом нижнем углу экрана почтовой системы. Размер: 90x30 пикселей, фон: прозрачный.

- **customlogomedium.png**

Логотип CommuniGate Pro с обрамлением на странице входа. Размер: 145x50 пикселей, фон: прозрачный.

Почта к нам и от нас

Общие рекомендации

Чтобы почта с сервера доходила до адресатов в интернете:

- все ip-адреса почтовых релеев должны быть обязательно прописаны в обратной dns-зоне;
- "Greeting name" почтового сервера должен соответсвовать его dns-имени;
- необходимо читать сообщения, приходящие на abuse@, и своевременно на них реагировать;
- уменьшить время повторов посылки и увеличить количество попыток хотя бы для первого часа, это поможет уменьшить задержки до севреров, использующих greylisting. При времени повтора 1 час и выше почта рискует быть доставленной не за одни сутки;

В качестве рекомендуемой меры можно зарегистрировать свою сеть (или конкретно почтовые сервера) в DNSWL и EmailReg.org

Однако следует понимать, что всегда в интернете найдется сервер который не захочет принимать почту от нас. Авторам в свое время попался американский почтовый сервер, возвращавший письма с объяснением вида "550 E-mail from Russia. Bye!"

Стандартные e-mail адреса

Для взаимодействия с сетью интернет серверу крайне желательно содержать определенное число стандартных адресов[21] (RFC 2142).

В нашем случае используются адреса:

- abuse@ и postmaster@ для жалоб
- webmaster@ для обратной связи с сайтов (RFC 2068)
- info@ по общим вопросам
- noc@ и support@ для связи с техперсоналом
- hostmaster@ для вопросов, связанных с DNS (RFC 1033 - RFC 1035)
- clockmaster@ для вопросов, связанных с сервером NTP

SPF записи в DNS

Для домена [22]:

```
example.com.      IN TXT           "v=spf1 mx ~all"
```

Для почтового сервера:

```
mail              IN TXT           "v=spf1 a -all"
```

Это поможет пользователям получать почту от нас.

Так же можно воспользоваться мастером содания SPF-записей от компании Microsoft:

- http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/default.aspx

Как посмотреть кто и куда звонил?

```
grep "out call completed" /var/CommuniGate/SystemLogs/*.log
```

Как посмотреть на какие домены шлют почту пользователи?

Просто список доменов (для скриптов):

```
grep 'SMTP.\+sent to.\+got:250' /var/CommuniGate/SystemLogs/*.log | awk -F "[ ,(,)]" '{ print $4; }' | sort | uniq
```

Список доменов, наглядный с числом отосланных писем (для отчетов):

```
grep 'SMTP.\+sent to.\+got:250' /var/CommuniGate/SystemLogs/*.log | awk -F "[ ,(,)]" '{ print $4; }' | sort | uniq -c | sort -r
```

Десятка самых популярных доменов:

```
grep  'SMTP.\+sent to.\+got:250' /var/CommuniGate/SystemLogs/*.log | awk -F "[ ,(,)]" '{ print $4; }' | sort | uniq -c | sort -r | awk '{ print $2;  }' | head
```

Как посмотреть куда ломятся вирусы и спамботы?

```
grep 'SMTPI.\+unknown user account' /var/CommuniGate/SystemLogs/*.log | awk
```

```
'{ print $5; }' | sort | uniq -c | sort -d
```
То же самое но десятка лидеров:

```
grep 'SMTPI.\+unknown user account' /var/CommuniGate/SystemLogs/*.log | awk
'{ print $5; }' | sort | uniq -c | sort -d | head
```

С каких серверов чаще всего письма приходят в СПАМ

> **ВНИМАНИЕ!**
> Команда неоптимизирована и выполняется достаточно долго.
> Другие варианты приветствуются на странице обсуждения статьи.

```
find  /var/CommuniGate/Domains/example.com/ -type f |grep "SPAM.mdir"| xargs
head -n 30 | grep "Received: from "|awk '{ print $3; }'|sort|uniq -c |  sort -r
```

Смотрим, какие сервера используются RPOP

```
grep "RPOP-" /var/CommuniGate/SystemLogs/*.log | awk -F "[ ,(,)]" '{ print
$4; }'|sort|uniq -c
```

Как проверить, какие MX не хотят принимать почту от нас

```
grep  "Expected 25x <id>, got:550" /var/CommuniGate/SystemLogs/* | awk  -F
"[(,)]" '{ print $2; }' | sort | uniq -c | sort -n -r
```

Как узнать кому приходят письма с определенного адреса

/usr/local/bin/cgp-whoreceived.sh

```
#!/bin/bash

# Logfile name
WER="2011-10-19.log"

# e-mail address of a message
WHO="exampleuser@example.org"

WUT=`grep $WHO /var/Communigate/SystemLogs/$WER | grep QUEUE | awk '{ print
$3; }' | tr -d "[]" | awk -F "[(,)]" '{ print $2; }'`

for i in $WUT
do
 grep $i $WER | grep DEQUEUER | awk -F "[(,)]" '{ print $2; }'
done
```

Проверка ip-адреса почтового сервера на наличие в RBL

В сети интернет существует большое число утилит для удобной проверки адресов на попадание в RBL. Можно воспользоваться как одним из on-line сервисов вроде OpenRBL так и скриптами, выполняемыи непосредственно на сервере, к примеру RBLLookup Version 1. Для работы программы необходимы prel-модули

- Net::DNS
- Term::ANSIColor

которые легко устанавливаются через CPAN.

Программа работает следующим образом, из командной строки указываем какой адрес проверить:

```
./rbl.pl 198.51.100.92
```
и ждем результата.

Так же существуют плагины для подключения к Nagios

Онлайн-ресурс для проверки включения в RBL: MultiRBL

Проверка сервера на Open Relay

Для проверки сервера на открытый релей можно пользоваться сайтом http://www.nettools.ru/

Решение проблем

В LDAP-справочнике отсутствует существующий в системе пользователь

Иногда случается, что в Справочнике либо не отображается существующий пользовать, либо наоборот, в выдаче присутствует удаленный человек. Это означает, что произошла рассинхронизация Справочника и данных Домена (не Directory-based).

Вылечить можно, пересоздав записи в справочнике. Идем:

Пользователи -> Домены -> example.com -> Установки Домена -> Центральный Справочник

Нажимаем по очереди на кнопки "Стереть Все Записи" и "Создать Все Записи".

Не загружается веб-интерфейсе Pronto! с ошибкой #2036

Выставьте верную дату и время на ПК, либо синхронизируйте с ntp. Сбросьте кэш и настройки браузера.

Не прикладываются файлы в веб-интерфейсе Pronto! с ошибкой #2038

Симптомы: файл не прикладывается, ssl-сертификат импортирован в локальное хранилище, размер файла не превышает разрешенный для данного пользователя (домена).

Решение: проверить *Ограничение размера Запроса* на вкладке *Установки -> Услуги -> HTTPU* Оно д.б. => установленного лимита на размер файла в домене.

В IE8 веб-интерфейс Pronto! не грузится с ошибкой #2048

При этом есть свободное место на диске

Решение: очистите IE8 в меню *Сервис > Свойства обозревателя > Дополнительно > Сброс*

Коды ошибок почтовых серверов

RFC 3463 регламентирует номер кодов ошибок, которыми почтовая система информирует отправителя о недоставке [23] письма получателю, к примеру:

- 5.1.1 (Unknown user),
- 5.2.2 (Mailbox full)
- 5.7.1 (Rejected by security policy/mail filter)

http://www.answersthatwork.com/Download_Area/ATW_Library/Networking/Network__3-SMTP_Server_Status_Codes_and_SMTP_Error_Codes.pdf

"docx" файлы открываются как zip-папки

Необходимо добавить следующие mime-типы в разделе *Установки — Услуги — HTTPU — MIME-типы :*

```
".manifest", "application/manifest"
".xaml", "application/xaml+xml",
".application",  "application/x-ms-application",
".deploy", "application/octet-stream"
".xbap", "application/x-ms-xbap"

".docm","application/vnd.ms-word.document.macroEnabled.12"
".docx","application/vnd.openxmlformats-
officedocument.wordprocessingml.document"
".dotm","application/vnd.ms-word.template.macroEnabled.12"
".dotx","application/vnd.openxmlformats-
officedocument.wordprocessingml.template"
".potm","application/vnd.ms-powerpoint.template.macroEnabled.12"
".potx","application/vnd.openxmlformats-officedocument.presentationml.template"
".ppam","application/vnd.ms-powerpoint.addin.macroEnabled.12"
".ppsm","application/vnd.ms-powerpoint.slideshow.macroEnabled.12"
".ppsx","application/vnd.openxmlformats-
```

```
officedocument.presentationml.slideshow"
".pptm","application/vnd.ms-powerpoint.presentation.macroEnabled.12"
".pptx","application/vnd.openxmlformats-
officedocument.presentationml.presentation"
".xlam","application/vnd.ms-excel.addin.macroEnabled.12"
".xlsb","application/vnd.ms-excel.sheet.binary.macroEnabled.12"
".xlsm","application/vnd.ms-excel.sheet.macroEnabled.12"
".xlsx","application/vnd.openxmlformats-officedocument.spreadsheetml.sheet"
".xltm","application/vnd.ms-excel.template.macroEnabled.12"
".xltx","application/vnd.openxmlformats-officedocument.spreadsheetml.template"
```

Hotmail.com

```
Failed to deliver to 'user1@hotmail.com'
SMTP module(domain hotmail.com) reports:
 return-path address <user2@example.com> rejected by mx4.hotmail.com:
 550 SC-001 (BAY0-MC1-F7) Unfortunately, messages from 192.0.2.10 weren't sent.
 Please contact your Internet service provider since part of their network is
on our block list.
 You can also refer your provider to http://mail.live.com/mail/
troubleshooting.aspx#errors.
```

Необходимо открыть тикет:

- https://support.msn.com/default.aspx?productKey=edfsmsbl&locale=en-us&st=1&wfxredirect=1

Ошибка HTTPU failed to pass I/O subsystem to the Dispatcher

HTTPU модуль принимает на свои сокеты соединения и других протоколов, а именно - XIMSS. Когда по данным в соединении становится ясно, что обрабатывать соединение должен модуль XIMSS (а не модуль HTTPU, который соединение принял), это соединение передаётся для обработки другому модулю. У вас же, похоже, модуль XIMSS принять соединение не может: из за ограничения на общее количество каналов или на количество соединений с одного IP адреса [24].

Рутина

Изменение настроек Real-Time

Для изменения параметров в меню *Объекты -> <uid> -> Real-Time -> Правила для Входящих Звонков* используется следующая команда CGP CLI [25]:

```
SETACCOUNTSIGNALRULES accountName newRules
 Use this command to set the Account Signal Rules.
 accountName : string
  This parameter specifies the name of an existing Account. The name can
include the Domain name (see above).
 newRules : array
  This array should contain the Account Signal Rules. All old Account Signal
Rules are removed.
```

> **ВНИМАНИЕ!**
> This command can be used by Domain Administrators only if they have the ""Разрешённые Правила для Звонков (SignalRulesAllowed) *access right*.

Управление аккаунтами

Управление аккаунтами пользователей осуществляется администраторами домена при помощи внешнего java-приложения [26]. java-библиотека и описание функций работы представлены на сайте производителя по адресу: http://www.stalker.com/CGJava/

Вспомогательные perl-скрипты

Сброс всем пользователям размера почтового ящика на установленный "По-умолчанию" в домене

```
#!/usr/bin/perl -w
```

```
use CLI;

my $cli = new CGP::CLI( { PeerAddr => 'cgp.example.com',
                          PeerPort => 106,
                          login    => 'postmaster',
                          password => 'abc123'
                          } )
        || die "Can't login to CGPro: ".$CGP::ERR_STRING."\n";

my $domList=$cli->ListDomains() || die "can't list domains";

foreach $domain (sort @$domList) {
  $AccountList = $cli->ListAccounts($domain)
                 || die "Error: ".$cli->getErrMessage.", quitting";
  foreach(keys %$AccountList) {
    $address = "$_\@$domain";
    print "$address\n";

    $cli->UpdateAccountSettings($address,{MaxAccountSize => 'Default'})
        || die "Error: ".$cli->getErrMessage.", quitting";
  }
}

$cli->Logout;
```

Удалить из очереди на отправку все письма, содержащие вхождение определенной строки

Если какой-то аккаунт был скомпрометирован и до изменения пароля успел накачать в очередь сервера тысячи спаммерских сообщений, удалить их можно след. скриптом:

```
#!/usr/bin/perl

use strict;
use Data::Dumper;
use CLI;

my $cli=new CGP::CLI( {
   PeerAddr => 'localhost',
   PeerPort => '106',
   login    => 'your-postmaster',
   password => 'your-password'} );

unless($cli) {
   die "Can't login to CGPro: ".$CGP::ERR_STRING;
}

my $dir = "/var/CommuniGate/Queue";

if(@ARGV!=1) {
 print "rejectSMTPQueue-by-string.pl -- Reject from Queue all messages
containing a given string\n";
 print "usage: rejectSMTPQueue-by-string.pl <string>\n";
 exit;
}

print "searching messages...\n";
my @lines = `grep -r -l '$ARGV[0]' $dir | grep msg`;
## my @lines = `cd $dir ; ls *.msg | xargs grep -l $ARGV[0]`;

my $count=0;

print "rejecting selected messages...";
foreach my $line (@lines) {
```

```
    $line =~ /([0-9]+)\.msg/;
    my $msg = $1;
    print "\n$msg ";
    my $ret = $cli->RejectQueueMessage($msg);
    if(!$ret) { print $cli->getErrMessage; next; }
    print "rejected";
    $count++;
}

# Close the CLI connection
$cli->Logout();

print "\n\nTotal: $count\n";
```

Второй вариант скрипта:

По отправителю

```
#!/usr/bin/perl -w
use CLI;
if (defined($ARGV[0]))
{
$user = $ARGV[0];
}
else
{
printf ("Wrong format\nUse delQ.pl sender_email\n");
exit;
}
my $cli = new CGP::CLI( { PeerAddr => 'hostname',
                          PeerPort => '106',
                          login    => 'postmaster@hostname',
                          password => 'password'
                          } )
        || die "Can't login to CGPro: ".$CGP::ERR_STRING."\n";
my @TMP = `grep -E -r "P*<$user>" /var/CommuniGate/Queue`;
foreach my $i (@TMP)
{
my $t = '^/var/CommuniGate/Queue/\d\d/(\d+).msg:P.+<'.$user.'>$';
if($i =~ /$t/)
 {
 $cli->RejectQueueMessage($1);
 printf ("#$1\n");
 }
}
$cli->Logout;
```

если по получателю поменять grep на

```
my @TMP = `grep -E -r "R*<$user>" /var/CommuniGate/Queue`;
```

и regexp проверки

```
my $t = '^/var/CommuniGate/Queue/\d\d/(\d+).msg:R.+<'.$user.'>$';
```

по IP отправителя

```
my @TMP = `grep -r '$user' /var/CommuniGate/Queue`;
```

и

```
my $t = '^/var/CommuniGate/Queue/\d\d/(\d+).msg:S\s+\S+\s+\['.$user.'\]';
```

по Hello

```
my @TMP = `grep -r "$user)" /var/CommuniGate/Queue`;
```

и

```
my $t = '^/var/CommuniGate/Queue/\d\d/(\d+).msg:Received:\s+from.+(HELO\s+'.
$user.'\s*)';
```

по from из заголовков

```
my @TMP = `grep -r "$user" /var/CommuniGate/Queue`;
```
и
```
my $t = '^/var/CommuniGate/Queue/\d\d/(\d+).msg:Received:\s+from.+\['.
$user.'\]';
```
Путь до очереди необходимо поправить на свой. Можно сделать разные файлы для каждого варианта.

Работа с пользователями

FAQ для пользователей: CommuniGate_FAQ

FAQ по использованию сервиса от компании Zenon N.S.P. http://www.go.ru/faq.html

Еще о том-же для администраторов сервисов: http://www.host.ru/support/mail/

FAQ почтовой службы Rambler: http://help.rambler.ru/project.html?s=103

Примеры документации для пользователей (нужное!!!): http://unixgeek.nm.ru/guides.html

Списки рассылки

Использование символа "-" в именах списков строго не рекомендуется[27].

Меняем владельца списка рассылки

Это давняя проблема Communigate. Непонятны трудности, из-за которых она до сих пор не решена, но это должно быть довольно сложно, ведь учитывая количество версий, разработчики продолжают игнорировать просьбы клиентов хоть как-то решить эту проблему.

1. Воспользуйтесь интерфейсом администратора по адресу http://mail.example.com:8010
2. В аккаунте нового владельца создайте новый список рассылки с названием mailing-list-name_new.
3. В данных почтового сервера domains/example.com/lists, скопируйте mailing-list-name.* mailing-list-name_new.*0
4. Измените настройки mailing-list-name_new.
    1. Найдите строку owner = old-owner и замените old-owner на new-owner
    2. Сохраните изменения и выйдите.
5. Используйте веб-интерфейс почты для аутентификации под аккаунтом старого владельца
6. Выберите папку в качестве списка рассылки
7. Выберите настройки для этой папки
8. Добавьте нового владельца со всеми правами доступа и примените для всех подпапок
9. Выйдите из аккаунта
10. Войдите в систему как новый владелец
11. Добавьте алиас для старого списка рассылки *~owner-name/mailing-list-name*
12. Скопируйте содержимое этой папки и всех подпапок в новый список рассылки
13. Вернитесь назад и удалите алиас
14. Проверьте настройки и список подписчиков, чтобы убедиться, что все в порядке (нажмите Настройки рядом со списком папок).
15. Выйдите из аккаунта
16. Снова войдите как администратор
17. Переименуйте старый список в mailing-list-name_old
18. Переименуйте новый список в mailing-list-name
19. Удалите старый список.

Графики работы сервера через MRTG

Оригинальная инструкция: http://www.communigate.com/CGMRTG/

В административном интерфейсе cgp *Установки -> Услуги -> SNMP* вбиваем пароль "public", затем на вкладке приемник выставляем:

```
Порт: 161
```

```
Локальный Сетевой Адрес: 127.0.0.1
Ограничения на удалённые Сетевые Адреса: Нет
```
Устанавливаем пакет mrtg:
```
zypper in mrtg
```
Создаем папку */etc/mrtg* куда скачиваем файл http://www.communigate.com/CGMRTG/mrtg.cfg и переименовываем его в cgp.cfg:
```
mkdir /etc/mrtg
cd /etc/mrtg
wget http://www.communigate.com/CGMRTG/mrtg.cfg
mv mrtg.cfg cgp.cfg
```
Правим файл. Удаляем строки:
```
RunAsDaemon: Yes
Interval: 5
```
Заменяем все <community>@<ip> на public@127.0.0.1

В каталоге */usr/local/sbin/* создаем файл *run_mrtg_cgp.sh* следующего содержания:
```
#!/bin/bash
env LANG=C /usr/bin/mrtg /etc/mrtg/cgp.cfg
```
В каталоге */etc/cron.d/* создаем файл *mrtg*:
```
*/5 * * * * root /usr/local/sbin/run_mrtg_cgp.sh > /dev/null
```
Идем в папку */var/CommuniGate/Accounts/postmaster.macnt/account.web* и генерируем индексный файл:
```
cd /var/CommuniGate/Accounts/postmaster.macnt/account.web/
indexmaker --output=default.html --columns=1 /etc/mrtg/cgp.cfg
```
Если в настройках домена индексный файл для аккаунта postmaster установлен не default.html, то переименовываем его в необходимый.

Проверяем работу mrtg запустив
```
/usr/local/sbin/run_mrtg_cgp.sh
```
и зайдя браузером по адресу http://mail.example.com/~postmaster/

Должны появиться графики.

Настройка клиентских машин

- https://mail.communigate.com/~ab/files/LDAP-Clients-CGP.html

Расширение для Thunderbird:

- http://www.niversoft.com/wiki/index/SyncCGP

Для MS Outlook используем идущий в комплекте MAPI-плагин. Пример настройки клиента: Настройка Microsoft Outlook 2007

Интеграция

Внешняя аутентификация в Active Directory

- Статья Интеграция почтового сервера CommuniGate Pro с доменом Microsoft Active Directory[28]
- Статья CommuniGate Pro External Authentication[29]

Пользователь регистрируется в Active Directory (AD), авторизуется в почте - если это новый пользователь, то будет создана учетка в communigate.

1. Домены > example.com
2. Установки Домена > Неизвестные Имена, Обратиться к Помощнику для Неизвестных > Да
3. Умолчания для Пользователя > Установки > Аутентификация
    1. Через Внешнюю Программу > Включено
    2. Шифрование Пароля > не шифровать
4. **?** Далее жмём на галку в левом верхнем углу. В поле Display and Data Input устанавливаем

Charset=utf8-получаем корректное отображение имени пользователя, так как Windows Server 2003 использует ту же кодировку utf8.

5. Установки > Общее > Помощники > Внешняя Аутентификация, Путь к Программе

```
/usr/local/bin/authLDAPNewAD.pl
```

Примечания

1. ↑ SUSE® Linux Enterprise Server
2. ↑ IBM PowerVM. The virtualization platform for UNIX, Linux and IBM i clients
3. ↑ IBM System p. Серверы AIX и Linux
4. ↑ CommuniGate Pro platform
5. ↑ CommuniGate Pro Perl Interface
6. ↑ Cloudmark Plugin for CommuniGate Pro. Create the Scanning Rule
7. ↑ Simple Mail Transfer Protocol. Mail processing model
8. ↑ TCP/IP Ports for Internet Services
9. ↑ SPF website. How Does SPF Work?
10. ↑ Reverse DNS lookup. From Wikipedia, the free encyclopedia
11. ↑ The Spamhaus Project - ZEN
12. ↑ The CBL
13. ↑ Российская система Dial-up User List(DUL)
14. ↑ Rambler-mail: insecure-bl.rambler.ru lookup
15. ↑ dnswl.org - Protect against false positives
16. ↑ http://mx.demos.su/lists/cgp-russian/2009_11/16150.html
17. ↑ Communigate Pro (CGP, CGatePro) + DomainKeys +DKIM with Sign
18. ↑ https://support.communigate.com/kb_article.php?ref=4408-QSHK-1117
19. ↑ http://cgp.rsu.edu.ru:8010/Guide/russian/PBXApp.html
20. ↑ http://cgp.rsu.edu.ru:8010/Guide/russian/CGPL.html
21. ↑ Хабрахабр: Кое-что о соглашениях об именах почтовых ящиков / Системное администрирование
22. ↑ SPF: SPF Record Syntax
23. ↑ Non delivery report. From Wikipedia, the free encyclopedia
24. ↑ http://mx.ru/Lists/CGatePro/Message/19561.html?Skin=Russian
25. ↑ http://www.communigate.com/CommuniGatePro/CLI.html
26. ↑ ftp.rsu.edu.ru/pub/software/cgp/jAdmin/
27. ↑ Mailing List CGatePro@mx.ru Message 19141
28. ↑ http://xn--80akakbjcdfphdy1ackb4nd.xn--p1ai/in/CommuniGate%20Pro/integracia
29. ↑ http://www.communigate.com/CGAUTH/

См. также

- Linksys
- SuSE Linux
- Борьба с брутфорсом SSH

Ссылки по теме

Communigate

- http://www.stalker.com/
- http://lang.communigate.com/ru/
- https://support.communigate.com/howto/
- http://www.stalker.com/CGJava/
- http://www.stalker.com/CGPerl/
- ftp://ftp.stalker.com/pub/CommuniGatePro/
- http://unixgeek.nm.ru/
- http://www.mineralogist.ru/oder/communigate/

- http://forum.voxilla.com/communigate-pro-support-forum/
- http://forum.ru-board.com/topic.cgi?forum=5&topic=19377
- https://support.communigate.com/forum/
- http://www.osp.ru/text/print/302/4261.html
- communigate-cpanel-adaptor: An integration kit for CommuniGate Pro (c) into the cPanel (c) VPS manager

SIP/PBX

- http://www.e164.org/
- http://enum.org/
- http://enumquery.com/
- http://mail.communigate.com/~ab/files/25c634725ca170c2413d5ad5faf9a0ce-39.html
- http://freewind.habrahabr.ru/blog/89142/
- Jabber SRV record generator
- Check DNS SRV records for XMPP

Списки рассылки

- http://mx.demos.su/lists/cgp-russian/
- http://mx.ru/Lists/CGatePro/List.html?Skin=Russian
- http://mail.stalker.com/lists/cgatepro/
- http://mail.stalker.com/Lists/CGatePro/

Adobe AIR

- http://get.adobe.com/air/
- http://talktoip.com/pronto/pronto.air

Скрипты для cgp

- http://communigate.com/ScriptRepository/
- http://cgpro.servicemail24.com/
- http://www.niversoft.com/products/cgscripts/cgscripts
- http://kocmuk.ru/2010/06/08/find-attachments-cgp/

cgpav

- http://program.farit.ru/doc/cgpav-rus.html

SpamAssasin

- http://spamassassin.apache.org/
- http://sa-russian.narod.ru/

ClamAV

- http://www.clamav.net/
- ftp://ftp.suse.com/pub/projects/clamav/

Механизм проверки SPF

- http://www.openspf.org/
- http://www.host.ru/support/mail/spf.html
- http://www.spamtest.ru/document?pubid=16637&context=1
- http://ru.wikipedia.org/wiki/Sender_Policy_Framework
- http://company.yandex.ru/articles/spf.xml

Проверка на наличие адреса в RBL

- http://openrbl.org/

Разное

- Проверка валидности e-mail средствами PHP
- http://del.icio.us/foboss/cgp/
- http://robotstxt.org.ru/
- http://www.emailreg.org/
- http://www.barracudacentral.org/
- Is your docx file turning into a zip?

- http://en.wikipedia.org/wiki/Bounce_message
- http://www.niversoft.com/wiki/index/A_Good_Antispam_and_Antivirus_Setup

RFC

- RFC 1912
- RFC 2142
- RFC 3463

Всякое

PBX

```
ngrep -W byline port 5060
```

Смотрим, кто вообще пользуется IP-телефонией:

```
grep sip-gw.address * | grep PBXLEG|awk -F "impersonate=" '{ print $2; }'|awk -
F ";" '{ print $1; }'|sort|uniq -c|sort -n
```

почему у меня возникает ошибка касательно доступа к LDAP после обновления CommuniGate Pro до версии 5.1.8 или более поздней?

LDAP-XXXXXXX([XX.XX.XX.XX]) search failed. Error Code=insufficient directory access rights

По умолчанию, новые версии CommuniGate Pro не разрешают анонимный доступ к Каталогу LDAP. Помимо записей журнала по данному вопросу, вы скорее всего найдете запись в журнале для этой же транзакции, которая демонстрирует попытку привязаться к Каталогу LDAP как 'anyone', то есть анонимно. Если вам нужно разрешить 'anyone' просмотр Каталогов LDAP, вам необходимо изменить права доступа к LDAP с помощью CGP Admin interface. Попав в раздел Directory | Access rights, вы скорее всего обнаружите тип прав 'ReadAll'. Если вы смените BindDN для этих прав с '*' на 'anyone', то анонимный доступ к Каталогу LDAP заработает.

Заметка о безопасности: Анонимный доступ к директории означает, что кто угодно может подключиться к вашему серверу и просматривать содержимое директорий через LDAP. Пожалуйста, имейте это ввиду при изменении настроек.

Автоматический редирект с http на https

Это может быть сделано посредством изменения вашей страницы аутентификации (login.wssp). Поместите это в самое начало файла:

```
< !--%%IF NOT(secureChannel)--><REDIRECT>https://yourdomain:9100< !--%%ELSE-->
... rest of login page
< !--%%ENDIF-->
```

Но вы не перенаправите и не обслужите страницу аутентификации через https. Вы можете запросто исправить атрибуты события Формы для того, чтобы данные при аутентификации могли бы передаваться через https. (почтовая веб-сессия завершится в режиме httpd). Просто найдите объявление <form> в login.wssp и измените обработчик как показано ниже.

```
<form action="https://yourdomain:9100" ... >
```

Perl

```
# ConvTime(string)
# This procedure converts CGPro textual date/time string into UNIX format
# (the number of seconds since 00:00:00 UTC, January 1, 1970).

sub ConvTime {
  my ($sec,$min,$hour,$mday,$month,$year);
  my %mNames=qw(Jan 0 Feb 1 Mar 2 Apr 3 May 4 Jun 5
                Jul 6 Aug 7 Sep 8 Oct 9 Nov 10 Dec 11);
  if($_[0] =~ /(\d{1,2}).(\w\w\w).(\d\d\d\d).(\d\d):(\d\d):(\d\d)/) {
    $mday=$1;
```

```
    $month=$mNames{$2};
    $year=$3-1900;
    $hour=$4;
    $min=$5;
    $sec=$6;
  } elsif($_[0] =~ /(\d\d)-(\d\d)-(\d\d\d\d).(\d\d):(\d\d):(\d\d)/) {
    $mday=$1;
    $month=$2-1;
    $year=$3-1900;
    $hour=$4;
    $min=$5;
    $sec=$6;
  } elsif($_[0] =~ /#T(\d\d)-(\d\d)-(\d\d\d\d)_(\d\d):(\d\d):(\d\d)/) {
    $mday=$1;
    $month=$2-1;
    $year=$3-1900;
    $hour=$4;
    $min=$5;
    $sec=$6;
  } else {
   die "Unknown date format: \"$_[0]\", quitting";
  }
  return POSIX::mktime($sec,$min,$hour,$mday,$month,$year);
}
```

BIND NAPTR DNS конфигурация для ENUM с расширениями

это содержимое для x.x.x.x.e164.arpa файла

```
$TTL 1800
@ IN SOA ns.core.at. hostmaster.xx.xx. (
                2007070801
                10000
                3600
                604800
                1800)


@               IN NS  ns.xx.xx.
                IN NS  ns2.xx.xx.

@ IN NAPTR 5 10 U E2U+sip "!^.*$!sip:pbx@SIPHOST!".
@ IN NAPTR 5 15 U E2U+email:mailto  "!^.*$!mailto:pbx@SIPHOST!".
@ IN NAPTR 5 20 U E2U+web:http "!^.*$!http://www.xxx.com!".
@ IN NAPTR 10 10 U E2U+tel "!^.*$!tel:\+43xxxxxx!".
*.0.1.0.1.0.8.0.8.7.3.4.e164.arpa. IN NAPTR 5 10 U E2U+sip "!^\\+43xxxxxx([0-9]
[0-9])$!sip:\\1@SIPHOST!".
*.0.1.0.1.0.8.0.8.7.3.4.e164.arpa. IN NAPTR 10 10 U E2U+tel "!^\\
+43xxxxxx([0-9][0-9])$!tel:\+43xxxxxx\\1!".
```

замените SIPHOST с FQDN вашего сервера (for example sip.core.at) замените +43xxxxx вашим enum-номером (+43780801010)

С такой конфигурацией вы получите расширения от 01 до 99 - если вам нужно добавить больше одного раза [0-9] в NAPTR-запись.

- https://support.communigate.com/forum/showthread.php?t=16

	[+] **Сеть**

Оборудование	СХД • Cisco • 3G модем • Vyatta
Active Directory	Group Policy (GPO) • LOCAL.RSU.EDU.RU • MSI • Windows Server 2008 • Миграция учетных записей
Службы	MnoGoSearch • Установка Netatalk (AFP) на OpenSUSE • Сервер точного времени ntp.rsu.edu.ru • Резервное копирование • Обновление Консультант + через интернет • Pdns • Nslookup • IIS • Group Policy (GPO) • DNS & DHCP • BGP • OSPF
Программное обеспечение	Консоль управления PERCo-S-20 • Антивирус Касперского • Windows XP • Windows Server 2008 • Vyatta •Google Chrome • **Communigate Pro** • Bacula • Ulteo Open Virtual Desktop • 1C
Настройка	Типичная настройка сети университета • Подключение к сети университета через VPN • Публичная Wi-Fi сеть РГУ• Настройка сетевого оборудования • Настройка сервера DNS • Настройка web-сервера • Настройка proxy-сервера • Автоматическая настройка прокси • Внедрение IPv6

	[+] **Платформа унифицированных коммуникаций**
Почта	Настройка Apple Mail 3.0 • Настройка Opera Mail • Настройка почтовых клиентов • Настройка Microsoft Outlook 2003 • Настройка Microsoft Outlook Express • Настройка Microsoft Outlook 2007 • Настройка Novell Evolution•Сбор почты с внешних POP3 серверов • Правила электронной переписки
IP телефония	Настройка IP-телефонов • IP-телефон (Софтофон) для ПК и Смартфонов • Настройка голосовой почты и переадресации звонков • Linksys • Gigaset • Cisco (IP-телефон) • Astra (IP-телефон) • Настройка CounterPath X-Lite • Настройка SIP-клиента Windows Messenger 5.1• Справочник IP-номеров
Платформа CommuniGate	**Communigate Pro** • CommuniGate FAQ • Документооборот на платформе CommuniGatePro • Communigate Pro 5.2