

Настройка Mail Proxy для GroupWise

Куличкин Виктор

CNE

<http://kvy.marka.net.ua>

Если кто-то утверждает, что он сможет ввести в эксплуатацию новый продукт Novell, используя только пришедшую с ним документацию, то здесь я соглашусь с трудом. Но если стоит вопрос о стыковке двух систем Novell, тогда никто меня не убедит, что без использования дополнительных источников информации здесь не обойтись. В качестве примера можно привести организацию работы GroupWise через BorderManager.

Несмотря на кажущуюся простоту описания процедур по установке сервисов в этих системах, практическая реализация их содержит множество «подводных камней», на обход которых необходимо затратить дополнительное время. А именно, пуститься на долгие поиски и изучения соответствующих Информационных Документов (TID) на <http://support.novell.com>. Поэтому я решил написать статью, в которой собрана вся необходимая информация для стыковки этих двух систем. Надеюсь, что приведенная здесь методика поможет моим коллегам избежать трудностей, с которыми я столкнулся при реализации этого проекта.

Перед тем, как приступить к описанию, я счел нужным сообщить, что все мои решения основаны на Информационных Документах Novell (TID), регистрационные номера которых приведены перед каждой установкой. Следовательно, если у вас в ходе изучения этого материала возникнут сомнения по поводу того или иного действия, тогда вы всегда можете обратиться к первоисточнику, найдя его на <http://support.novell.com>

Постановка задачи

Для сервера с GroupWise 5.5.5, установленного в локальную сеть предприятия, необходимо обеспечить прохождение электронной почты в/из Интернет. Связь локальной сети с Интернетом осуществляется через отдельный сервер, на котором установлен BorderManager 3.6 с Support Pack 1a и Update bm36c02.exe. В качестве операционной системы на обоих серверах используется NetWare 5.1 с Support Pack 2a.

Для обмена электронной почтой с Интернетом на GroupWise сервере устанавливается GroupWise Internet Agent (в дальнейшем GWIA), а на BorderManager сервере – Mail Proxy (в дальнейшем Почтовый прокси). Задача этого проекта состоит в настройке GWIA и Почтового прокси для их совместной работы.

Установка Почтового прокси

Перед тем как начать установку, вы должны знать, что Почтовый прокси - это единственный из сервисов BorderManager'a, за которым тянется длинный «хвост» недоработок. Поэтому вам необходимо установить все последние изменения на BorderManager сервер с <http://support.novell.com/misc/patlst.htm>.

Установка прокси выполняется по TID 10023303. В соответствии с этим документом в NWADMIN войдите в “Details” BorderManager сервера и выберите “BorderManager Setup”. Затем включите “Mail Proxy” и через кнопку “Details” вызовите конфигурационное окно Почтового прокси. В этом окне необходимо заполнить следующую информацию.

Spool Directory. Здесь необходимо указать путь к каталогу Почтового прокси. В нем будут созданы подкаталоги для входящих (INCOMING) и исходящих (OUTGOING) сообщений. Следовательно, том сервера, на котором будут созданы каталоги, должен иметь достаточно места для размещения этих сообщений. По умолчанию выбирается SYS:\ETC\PROXY\SPOOL.

Spool Directory Max Size. Выберите 4000 Mb.

Max Mail Size. Выберите 2000 Mb.

Эти значения выбраны в соответствии с TID 10023303. Novell предупреждает, что если в Почтовый прокси попадает сообщение, размер которого превышает значения, указанные в Spool Directory Max Size и Max Mail Size, тогда сервер зависает или выходит в abend. Поэтому вы должны выбрать именно эти значения, даже если размер тома не позволяет сделать этого.

Failed Mail Retry Interval. Оставьте по умолчанию – 10 мин.

Failed Mail Retry Count. Я предлагаю установить максимальное значение – 20.

Primary Mail Domain Name. Укажите имя вашего почтового домена. Например, yourdomain.com.

Internal Mail Server. Укажите внутренний IP адрес вашего GroupWise сервера.

POP3 Mail Server Name. Укажите внутренний IP адрес вашего GroupWise сервера.

Установка правил доступа для Почтового прокси

Novell по этому поводу немногословен. Все, что мне удалось найти - это краткая запись в TID 10014027, которая говорит, что правила доступа (Access Control Rules) должны быть достаточными для прохождения сообщений через прокси. А также иметь следующие характеристики:

Access Type: Application Proxy

Access Details: SMTP Mail

Ну что ж, сказано ясно и содержательно. Поэтому я беру на себя смелость и развиваю эту идею дальше. Для того чтобы ваша почта проходила через Почтовый прокси, вы должны установить три правила:

- Вашему GroupWise серверу (вашей подсети) разрешено посылать почту в Интернет, используя порт 25.
- Позволить всем посылать почту в ваш почтовый домен.
- Заблокировать весь 25 порт для предотвращения прохождения spam'а через прокси.

Практическая реализация этих правил будет выглядеть следующим образом (напомню, что правила доступа создаются в NWADMIN: ваш BorderManager сервер | Details | BorderManager Access Rules):

1. Правило на передачу сообщений:

- Action: Allow
- Access Type: Port
- Service: SMTP
- Origin Server Port: 25
- Transport: TCP, UDP
- Source: Specified – IP адрес вашего GroupWise сервера
- Destination: Any

2. Правило на прием сообщений:

- Action: Allow
- Access Type: Application Proxy
- Proxy: SMTP
- Source: Any
- Destination: Specified – имя вашего почтового домена (Например, yourdomain.com).

3. Правило на блокировку порта 25:

- Action: Deny
- Access Type: Port
- Service: SMTP
- Origin Server Port: 25
- Transport: TCP, UDP
- Source: Any
- Destination: Any.

PROXY.CFG

Этот файл размещается в каталоге SYS:\ETC\PROXY вашего BorderManager сервера и содержит дополнительные конфигурационные установки для всех его прокси. Однако по отношению к Почтовому прокси есть небольшая особенность. TID 10023303 требует вручную добавить дополнительную секцию в этот файл. Это утверждение справедливо для BorderManager 3.5, 3.6 и 3.7. Пример такой секции приведен ниже:

```
[BM Mail Proxy]
BM_Domain=yourdomain.com
BM_Incoming_Relay=0
BM_Proxy_Domain=mail-proxy.yourdomain.com
```

BM_Domain. Здесь необходимо указать имя вашего зарегистрированного домена (например, yourdomain.com). Это значение используется прокси для проверки поступающей почты на spam relay. Т.е. если имя домена в поле TO поступающего сообщения не одинаково с именем вашего домена, тогда прокси отбрасывает это сообщение. Значение в BM_Domain не требуется, если вы указали его в NWADMIN в Primary Domain Name (см. раздел «Установка Почтового прокси»).

BM_Proxy_Domain. Это поле содержит DNS имя вашего BorderManager прокси и используется им при формировании HELO команд для SMTP сервера. Это свойство применяется при проверке на spam, когда SMTP сервер-адресат проводит DNS идентификацию вашего узла при получении почты от него. Заполнять это поле необязательно, но я рекомендую указать здесь значение, если вы не хотите, чтобы часть вашей почты было отброшено другими серверами.

BM_Incoming_Relay. Это поле может содержать только два значения: 0 или 1. Если поле содержит 1, тогда Почтовый прокси может перенаправлять (relay) почту, содержащую знак “%”. Например, если пришедшее сообщение в TO ADDRESS содержится запись john DOE%abc.com@yourdomain.com, тогда ваш прокси перенаправит его по адресу john DOE@abc.com. Следовательно, вы подготовили неплохую базу для прохождения spam’a. Поэтому Novell рекомендует в поле BM_Incoming_Relay устанавливать 0, что заставляет Почтовый прокси не принимать почту со знаком “%”.

Установка фильтров для Почтового прокси

Здесь необходимо использовать TID 10014028 (или 10020917). Все настройки проводят с консоли BorderManager сервера через FILTCFG.NLM. Последовательность установки фильтров следующая.

Загрузите FILTCFG, затем выберите Configure TCP/IP Filters | Packet Forwarding Filters | Exceptions, после нажать кнопку “Insert” и ввести следующую информацию:

- Source Interface Type: Interface
- Source Interface: введите имя вашей платы для public сети
- Destination Interface Type: Interface
- Destination Interface: All interfaces
- Packet Type: SMTP
- Protocol: TCP
- Destination Port(s): 25
- Source Port(s): All
- Source Address Type: Any Address
- Destination Address Type: Host
- Destination Address: IP адрес вашего GroupWise сервера

Выйдите из FILTCFG и для активизации новых записей в фильтрах выполните ряд команд на консоли сервера:

```
UNLOAD IPXFLT
UNLOAD IPFLT
UNLOAD FILTSRV
REINITIALIZE SYSTEM
```

Следующая установка не относится к фильтрам и ее необходимо провести, если у вас на BorderManager установлен NAT. В соответствии с TID 10023303 на консоли сервера выполните команду:

```
SET NAT DYNAMIC MODE TO PASS THRU = ON
```

Это позволит через NAT получить доступ к портам 1 – 1023 (TID 10063019). В дальнейшем эту команду необходимо поместить в AUTOEXEC.NCF.

Настройка GWIA

Инсталляция GWIA не вызывает особых трудностей и выполняется по документации на GroupWise. Но для работы с Почтовым прокси в NWADMIN для GWIA необходимо установить два параметра (TID 10014027):

1. Имя в поле Foreign ID (Чужеродный ИД – для русской версии GroupWise) должен быть таким же, что и в поле Primary Mail Domain Name для Почтового прокси (см. раздел «Установка Почтового прокси»).
2. Ключ “/mh-IP адрес” GWIA.CFG должен указывать на внутренний IP адрес вашего BorderManager сервера. Этот ключ можно установить двумя способами:
 - Отредактировать файл GWIA.CFG вручную. Напомню - этот файл находится в каталоге WPGATE\GWIA. После установки ключа не забудьте перезагрузить GWIA.

- Или установить этот IP адрес через NWADMIN (TID 10009583):
GWIA | Details | SMTP/MIME Setting | Relay host for outbound messages
(Промежуточный узел исходящих – для русской версии GroupWise).

Быстрая проверка работы Почтового прокси

Выполняется по TID 10014027 при помощи Telnet. Для этого необходимо подсоединиться к внешней стороне вашего BorderManager сервера и открыть Telnet сессию через порт 25. Если Почтовый прокси сконфигурирован правильно, тогда вы должны получить сообщение:

“220 Service Ready”

Введите: “helo Novell.com” (заметьте в слове “helo” нет опечатки). Вы должны получить следующий ответ:

“250 yourdomain.com OK”

Введите: “mail from: your.mail@yourdomain.com”. Должен быть ответ:

“250 OK Requested Mail Action Complete”

Введите: “rcpt to: user@yourdomain.com”. Должен быть ответ:

“250 OK Requested Mail Action Complete”

Введите: “data” и напечатайте ваше сообщение. В конце сообщения – Enter, далее введите “.” и снова Enter.
Должен быть ответ:

“250 OK Requested Mail Action Complete”

После этого пользователь с именем “user” должен получить ваше сообщение. Если этого не происходит, тогда вам необходимо проверить цепочку прохождения вашего сообщения, а именно:

- Корректность набора выше перечисленных команд.
- Правильность настройки фильтров BorderManager. Для этого попробуйте на короткое время отключить их с помощью команды UNLOAD IPFLT и повторить проверку.
- Наличие этого сообщения в каталоге SPOOL/INCOMING. Обычно файлы входящих сообщений здесь долго не задерживаются и сразу же передаются в GroupWise сервер. Проверьте еще раз настройку вашего прокси.

Дальнейшую проверку, естественно, проводят на действующем почтовом сервере. Мой совет, я не рекомендую использовать сервера, которые предоставляют «бесплатные» почтовые ящики, например, yahoo.com,

hotmail.com и т.д. А раз их сервис бесплатный, то никто вам не гарантирует, что ваша почта будет вовремя доставлена или принята этим сервером.

Дополнительные настройки Почтового прокси

Здесь приведено решение проблемы, с которой я столкнулся при реализации этого проекта. Эти настройки необходимо применять лишь в том случае, если последний сервис пак на BorderManager не решает эту проблему.

После установки Почтового прокси по выше указанной методике я не имел никаких проблем с приемом почты. Но этого нельзя сказать о выходящей почте. Часть сообщений прекрасно доставлялось к своим адресатам, а другая часть – безнадежно зависала в каталоге OUTGOING и единственным способом «выбросить» их оттуда – это была перегрузка BorderManager сервера. Я также заметил, что на отправку почты влияли три фактора:

- Зависали сообщения, размер которых превышал 40 Кб.
- Расстояние почтового сервера-адресата. Я не мог отсылать почту с прикрепленными файлами в Штаты.
- Когда загрузка моего Интернетовского канала превышала 80%.

Решение этой проблемы я нашел в статье ведущего специалиста по BorderManager Крейга Джонсона (Craig Johnson, “Making Mail Proxy Work More Reliably”, <http://nscsysop.hypermart.net/mailprxy.html>). Там он предлагает использовать Почтовый прокси только для входящих сообщений, а для отправки почты применять Dynamic NAT. Для этого вам необходимо сделать несколько доработок:

1. Включить Dynamic (или Dynamic & Static) NAT в INETCFG вашего BorderManager сервера.
2. Установить SMTP фильтр в FILTCFG.NLM:
 - Source Interface Type: Interface
 - Source Interface: введите имя вашей платы для private сети
 - Destination Interface Type: Interface
 - Destination Interface: введите имя вашей платы для public сети
 - Packet Type: smtp-st
 - Protocol: TCP
 - Destination Port(s): 25
 - Source Port(s): All
 - Source Address Type: Host
 - Source Address: IP адрес вашего GroupWise сервера
 - Destination Address Type: Any Address
3. Установить default gateway в GroupWise сервере на внутренний IP адрес вашего BorderManager сервера.

4. Убрать ключ “/MH” в GWIA.CFG (см. раздел “Настройка GWIA”). Это позволит GroupWise серверу посылать сообщения прямо через NAT, минуя прокси.
5. Необходимо обеспечить возможность для GroupWise сервера посылать DNS запросы к внутреннему DNS серверу или обеспечить их прохождения через NAT. В любом случае вы должны иметь возможность с GroupWise сервера выполнить ping по URL (например, www.novell.com).

Больше настроек оба сервера не требуют, и ваш прокси готов к приему почты.