Фильтры Postfix и регулярные выражения!

Что есть спам!

Фильтрация.

Доабавим строки в main.cf:

```
 header_checks = regexp:/etc/postfix/header_checks
body_checks = regexp:/etc/postfix/body_checks
```

Готовые регулярные выражения для фильтрации можно взять тут

Примеры содержимого body_checks:

REDIRECT sima_pupkin@mail.ru после 100% й проверки можно заменит на REJECT

Не забываем, что Postfix не умеет редиректить (REDIRECT) письма со своего доменного имени на своёже.

В целях проверки воспользуйтесть сторонним почтовым ящиком!

Блокируем **http://xukauqeb.com** в теле письма.

/^(|[^>].*)http://xukauqeb.com/ REDIRECT sima_pupkin@mail.ru

проверка работоспособности:

postmap -q "**http://xukauqeb.com**" regexp:/etc/postfix/body_checks

блокируем **www.masterclass.org.ua**
/^(|[^>].*)www.masterclass.org.ua/ REDIRECT sima_pupkin@mail.ru

проверка работоспособности:

postmap -q " **www.masterclass.org.ua**" regexp:/etc/postfix/body_checks

Block mail with really old dates
/^Date:.*200[0-9]/ REJECT Message header rejected [058] - Date too old!
/^Date:.*19[0-9][0-9]/ REJECT Message header rejected [059] - Date too old!

Keyword
#/^(|[^>].*)Cialis/ REDIRECT sima_pupkin@mail.ru
#/^(|[^>].*)CIALIS/ REDIRECT sima_pupkin@mail.ru

#VIVARIO
/^(|[^>].*)VIVARIO/ REDIRECT sima_pupkin@mail.ru

#RUCELF
/^(|[^>].*)RUCELF/ REDIRECT sima_pupkin@mail.ru

rolex or cartier
/^Subject:(.*)([rR][-\.]?[oO0][-\.]?[lL][-\.]?[eE][-\.]?[xX][\.?]?)|([cC][-\.]?[aA4][-\.]?[rR][-\.]?[tT][-\.]?[iI\|1]

 # viagra
Looks simular to my body_checks entry, with just '^Subject:.*' prefixing the string.
/^Subject:.*(VP[-]?RX|[vV][j_\-]?[iI1][j_\-]?[aA4@][j_\-]?[gG][j_\-]?[rR][j_\-]?[aA4@])/ REDIRECT

sima_pupkin@mail.ru

E-mail address

#unt.del@mail.ru

/^(|[^>].*)del\@mail\.ru/ REDIRECT sima_pupkin@mail.ru
#vivario@mail.ru
/^(|[^>].*)vivario\@mail\.ru/ REDIRECT sima_pupkin@mail.ru

#9617933@mail.ru
/^(|[^>].*)9617933\@mail\.ru/ REDIRECT sima_pupkin@mail.ru

Цифры и кириллица в фильтрах неработает!!!

#shamanbest@rambler.ru
/^(|[^>].*)shamanbest\@rambler\.ru/ REDIRECT sima_pupkin@mail.ru

http address

#http://xuxuqyaq.com
/^(|[^>].*)http:\/\/xuxuqyaq\.com/ REDIRECT sima_pupkin@mail.ru

#www.edipresse.ua
/^(|[^>].*)www\.edipresse\.com/ REDIRECT sima_pupkin@mail.ru

#http://louuvbep.com
/^(|[^>].*)http:\/\/louuvbep\.com/ REDIRECT sima_pupkin@mail.ru

#www.masterclass.org.ua
/^(|[^>].*)www\.masterclass\.org\.ua/ REDIRECT sima_pupkin@mail.ru

http tag
/^(|[^>].*)charset\=3Deuc\-kr/ REDIRECT sima_pupkin@mail.ru
/^(|[^>].*)charset\=euc\-kr/ REDIRECT sima_pupkin@mail.ru

oleg_mv@ua.fm
/^(|[^>].*)oleg_mv\@ua\.fm/ REDIRECT sima_pupkin@mail.ru
neo.olya@gmail.com
/^(|[^>].*)neo\.olya\@gmail\.com/ REDIRECT sima_pupkin@mail.ru
nata_2007@gala.net

/^(|[^>].*)nata_2007\@gala\.net/ REDIRECT sima_pupkin@mail.ru

# Клиент, подключившийся к серверу, может командой vrfy определить, существует ли заданный адрес в системе. Т.е. vrfy user@example.com. Поэтому отключаем такую возможность
disable_vrfy_command=yes
# При попытке клиента отправить письмо несуществующему юзеру Постфикс выдаст 550 (reject) с сообщением "user unknown in local recipient table" (или другой таблице). Отключаем, пусть Постфикс просто сообщает "user unknown"
show_user_unknown_table_name=no
# Требуем от клиента приветствия (HELO/EHLO). Все, кто подключается, должны представляться
smtpd_helo_required=yes
# Создаём класс, в котором будет разрешена отправка от имени своего домена (т.е. адрес отправителя user@mydomain.ru). Нужно для того, чтобы никто другой (спамеры, например) не отправляли почту с наших адресов
smtpd_restriction_classes=from_mydomain
# Описание этого класса. Разрешаем отправлять с доверенных сетей (прописанных в mynetworks) или прошедшим аутентификацию. Остальных отбрасываем
from_mydomain=permit_mynetworks, permit_sasl_authenticated, reject
# Теперь идут smtpd_..._restrictions в порядке, в котором они обрабатываются

Ограничения для этапа HELO/EHLO. Применяются к имени хоста, его айпи-адресу и приветствию HELO/EHLO.
smtpd_helo_restrictions=
Разрешаем доверенные сети
[пробел]permit_mynetworks,
Разрешаем тем, кто прошёл аутентификацию
[пробел]permit_sasl_authenticated,
Отбрасываем неправильное (несуществующее) имя хоста (например hjfhg.r)
[пробел]reject_invalid_hostname,
Отбрасываем не полностью определённое доменное имя хоста
[пробел]reject_non_fqdn_hostname,
Отбрасываем, если хост по HELO/EHLO не имеет A или MX записи в ДНС
[пробел]reject_invalid_helo_hostname
Ограничения для этапа MAIL FROM. Применяется ко всему предыдущему + имя отправителя
smtpd_sender_restrictions=
Отбрасываем не полностью определённое имя отправителя
[пробел]reject_non_fqdn_sender,
Отбрасываем отправителя с несуществующего домена
[пробел]reject_unknown_sender_domain,
Отбрасываем несуществующих отправителей
[пробел]reject_unlisted_sender,
Проверяем отправителя. Если с нашего домена, то проверим, находится ли он в доверенной сети или прошёл аутентификацию
[пробел]check_sender_access hash:/etc/postfix/mysenders
Разрешаем отправлять с доверенных сетей
[пробел]permit_mynetworks,
Разрешаем отправлять прошедшим аутентификацию
[пробел]permit_sasl_authenticated,
Ограничения для этапа RCPT TO. Применяется к предыдущему + имя получателя
smtpd_recipient_restrictions=
[пробел]reject_non_fqdn_recipient,
[пробел]reject_unknown_recipient_domain,
[пробел]reject_unlisted_recipient,
[пробел]permit_mynetworks,
[пробел]permit_sasl_authenticated,
Режект, если получатель отсутствует в списке нашего домена или списке пересылки. Чтобы сервер на стал открытым релеем
[пробел]reject_unauth_destination
Ограничения для этапа DATA
smtpd_data_restrictions=
Отвергаем запрос, когда клиент посылает команды SMTP раньше времени, ещё не зная, поддерживает ли Постфикс
[пробел]reject_unauth_pipelining,
Режект клиента с пустым именем отправителя, который отправляет сразу нескольким получателям

[пробел]reject_multi_recipient_bounce
Ограничиваем клиенты, которые могут запрашивать у Постфикс очистку очереди сообщений
smtpd_etrn_restrictions=
[пробел]permit_mynetworks,
[пробел]permit_sasl_authenticated,
[пробел]reject

Файл /etc/postfix/mysenders:
Те, кто отправляет письма от нашего домена, проверяются классом from_mydomain
mydomain from_mydomain

И говый конфиг без комментов

```
disable_vrfy_command=yes
show_user_unknown_table_name=no
smtpd_helo_required=yes
smtpd_restriction_classes=from_mydomain
from_mydomain=permit_mynetworks, permit_sasl_authenticated, reject
smtpd_helo_restrictions=
[пробел]permit_mynetworks,
[пробел]permit_sasl_authenticated,
[пробел]reject_invalid_hostname,
[пробел]reject_non_fqdn_hostname,
[пробел]reject_invalid_helo_hostname
smtpd_sender_restrictions=
[пробел]reject_non_fqdn_sender,
[пробел]reject_unknown_sender_domain,
[пробел]reject_unlisted_sender,
[пробел]check_sender_access hash:/etc/postfix/mysenders
[пробел]permit_mynetworks,
[пробел]permit_sasl_authenticated,
smtpd_recipient_restrictions=
[пробел]reject_non_fqdn_recipient,
[пробел]reject_unknown_recipient_domain,
[пробел]reject_unlisted_recipient,
[пробел]permit_mynetworks,
[пробел]permit_sasl_authenticated,
[пробел]reject_unauth_destination
smtpd_data_restrictions=
[пробел]reject_unauth_pipelining,
```

[пробел]reject_multi_recipient_bounce
smtpd_etrn_restrictions=
[пробел]permit_mynetworks,
[пробел]permit_sasl_authenticated,
[пробел]reject

Файл /etc/postfix/mysenders:
mydomain.ru from_mydomain

оригиналы и дополнения:

http://www.postfix.ru/viewtopic.php?t=23782&postdays=0&postorder=asc&start=15

http://www.postfix.ru/viewtopic.php?p=39514

http://www.postfix.ru/viewtopic.php?t=2236