Настройка BlackList, WhiteList, GreyList, DKIM, SPF, DMARC, автоблокировки сервера

Черный список

Присутствие IP-адреса, подсети или email-адреса означает, что данное соединение или сообщение будет отклонено.
Исключение:

- Авторизованное соединение;
- IP-адрес находится в списке полного доступа;
- IP-адрес, подсеть или email-адрес находится в белом списке;
- IP-адрес находится в списке "Другие серверы" в настройке миграции.

Содержание

Настройка BlackList, WhiteList, GreyList, DKIM, SPF, DMARC, автоблокировки сервера
Черный список
Белый список
Серый список
DKIM (DomainKeys Identified Mail)
  Генерация приватного ключа
  Генерация публичного ключа
  Пример записи в зоне DNS
SPF (Sender Policy Framework)
  Пример записи в зоне DNS
DMARC (Domain-based Message Authentication, Reporting and Conformance)
  Пример записи в зоне DNS
Автоблокировки

Белый список

Белый список имеет приоритет над черным списком.
Для сущностей, описанных в белых списках:

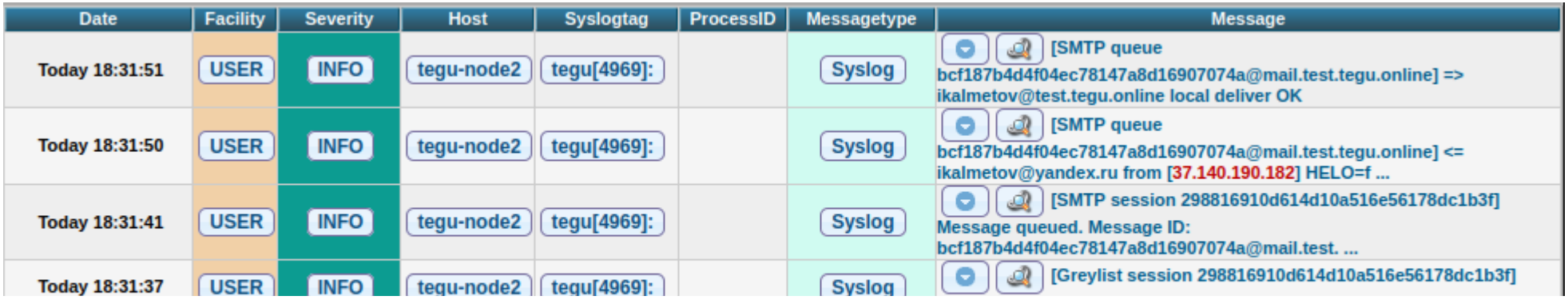
- Отменяется проверка SPF;
- Отменяется проверка DNSBL;
- Отменяется GreyList.

Серый список

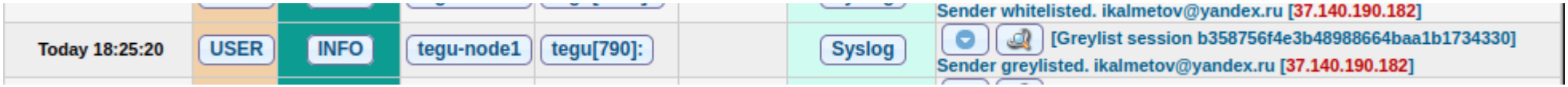
Greylisting — способ автоматической блокировки спама, основанный на том, что поведение спамерского сервера, оптимизированного на рассылки, отличается от поведения обычных серверов электронной почты.

Сервер, который использует Greylisting, отклоняет любое письмо от неизвестного отправителя, но при этом запоминает адрес отправителя. Смаперский сервер не повторяет попытки доставки, не смотря на то, что так положено по протоколу SMTP. Правильный сервер согласно RFC повторит попытку. В этом случае принимающий сервер найдет адрес отправителя в своих серых списках и незамедлительно примет письмо.

Вот как это выглядит в логе почтового сервера Tegu.



Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 18:31:51	USER	INFO	tegu-node2	tegu[4969]:		Syslog	[SMTP queue bcf187b4d4f04ec78147a8d16907074a@mail.test.tegu.online] => ikalmetov@test.tegu.online local deliver OK
Today 18:31:50	USER	INFO	tegu-node2	tegu[4969]:		Syslog	[SMTP queue bcf187b4d4f04ec78147a8d16907074a@mail.test.tegu.online] <= ikalmetov@yandex.ru from [37.140.190.182] HELO=f ...
Today 18:31:41	USER	INFO	tegu-node2	tegu[4969]:		Syslog	[SMTP session 298816910d614d10a516e56178dc1b3f] Message queued. Message ID: bcf187b4d4f04ec78147a8d16907074a@mail.test. ...
Today 18:31:37	USER	INFO	tegu-node2	tegu[4969]:		Syslog	[Greylist session 298816910d614d10a516e56178dc1b3f]



Разберемся:

- 18:25:20 - Входящее письмо с адреса ikalmetov@yandex.ru. Tegu отказывается принять письмо и помещает адрес отправителя в серый список.
- 18:31:37 - Повторная попытка отправки письма с адреса ikalmetov@yandex.ru. Tegu нашел пару IP адрес и email отправителя в серых списках, поэтому перемещает адрес в белые списки и принимает письмо.
- 18:31:51 - Обработка принятого письма завершена. Письмо доставлено получателю ikalmetov@test.tegu.online

Выводы:

- На сколько же затормозится доставка почты? Очевидно, что точный ответ на данный вопрос дать невозможно, т.к. это зависит не от Tegu, а от настроек отправляющего сервера. Обычно это несколько минут.
- Обратите также внимание, что сессия в 18:25:20 была инициирована с вычислительной нодой tegu-node1, а в 18:31:37 балансировщик отправил трафик на ноду tegu-node2. Однако, т.к. все сессии почтового кластера хранятся в единой БД, то вторая нода корректно отработала сессию, начатую первой нодой.
- Как показывает практика, долю нежелательной почты, которую удаётся отсечь с помощью Greylisting, достаточно велика. При этом ощутимо снизится и почтовый трафик, т.к., в отличие от анализаторов спама, приём спамерского сообщения не производится.
- Greylisting исключает ложные срабатывания, когда добропорядочное письмо блокируется фильтром и не попадает к адресату.
- Greylisting юридически чист. Блокирование почты на основании DNSBL, или прочтение почты анализаторами может вступить в определенное противоречие, но не Greylisting.

DKIM (DomainKeys Identified Mail)

DKIM RFC6376 - механизм, позволяющий проверить является ли отправитель достоверным или нет. Проверка осуществляется с помощью цифровой подписи, публичная часть которой находится в DNS соответствующей зоны. DKIM защищает от отправки сообщения с подменой адреса отправителя.

Чтобы настроить DKIM необходимо:

1. Создать пару (публичный/приватный) RSA-ключей;
2. Публичный ключ опубликовать в DNS-зоне;
3. Приватный ключ отдать своему серверу (он знает как с ним поступить).

Генерация приватного ключа

```
openssl genrsa -out private.pem 1024
```

Генерация публичного ключа

```
rsa -pubout -in private.pem -out public.pem
```

Пример записи в зоне DNS

Пример записи в зоне DNS

```
mail._domainkey.mbk-lab.ru.        IN    TXT    "v=DKIM1; h=sha256; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDIDhhzLlxzUP+49LDgA3xq9Xtre6yYCXoBFxk+vAPi
MkvWvZ4MAToJqWlJkYedMKWmyuelDX7KWHi1IVThxB1oNelG1q4H1dVg2BzpFSWx9+G1h/AOm08LxZxPb1
K57O2d44q6lrfNYijSA/99X+Jo0NDv2bO+MbdEg8Drp/w2bQIDAQAB"
```

где:

- mail — селектор;
- v — версия DKIM, всегда принимает значение v=DKIM1. (обязательный аргумент);
- k — тип ключа, всегда k=rsa. (по крайней мере, на текущий момент);
- p — публичный ключ, кодированный в base64. (обязательный аргумент).
- ; — разделитель.

Но в случае с почтовым сервером Tegu все обстоит намного проще.
Генерировать вручную RSA-ключ нет необходимости. Достаточно зайти в опцию меню **DKIM**, выбрать один из обслуживаемых сервером интернет-доменов и кнопкой **Создать** сгенерировать PSA-ключ. Приватную часть ключа сервер оставит себе, а публичную вернет вам для использования в описании DNS-зоны.

В дальнейшем, ключ можно пересоздать или удалить.

SPF (Sender Policy Framework)

SPF RFC7208 - механизм для проверки подлинности сообщения, путем проверки фактического адреса сервера отправителя со списком разрешенных адресов серверов, указанных в соответствующей зоне DNS. SPF не позволяет случиться ситуации, когда от имени вашего домена будут рассылаться мошеннические письма.

Пример записи в зоне DNS

```
mbk-lab.ru.        IN    TXT    "v=spf1 a mx -all"
```

Где:

- v=spf1 - является версией, всегда spf1;
- a - разрешает отправляет письма с адреса, который указан в A и\или AAAA записи домена отправителя;
- mx - разрешает отправлять письма с адреса, который указан в mx записи домена;
- all - означает то, что будет происходить с письмами, которые не соответствуют политике:
    - "-" — отклонять;
    - "+" — пропускать;
    - "~" — дополнительные проверки;
    - "?" — нейтрально.

DMARC (Domain-based Message Authentication, Reporting and Conformance)

DMARC RFC7489 — механизм снижения количества спамовых и фишинговых писем. DMARC описывает действие, которое должен совершить сервер для писем, которые не прошли проверку DKIM и SPF. А также описывает адрес, на который раз в сутки будет отправляться отчет об этих действиях.

Пример записи в зоне DNS

```
_dmarc.mbk-lab.ru.        IN    TXT    "v=DMARC1; p=quarantine; rua=mailto:abuse@mbk-lab.ru"
```

где:

- v - версия, принимает значение v=DMARC1 (обязательный параметр);
- p - правило для домена. Может принимать значения none, quarantine и reject, где:
  - p=none не делает ничего, кроме подготовки отчетов;
  - p=quarantine добавляет письмо в СПАМ;
  - p=reject отклоняет письмо;
- rua - позволяет отправлять ежедневные отчеты на email.

Автоблокировки

См. также:

- Включить систему защиты авторизации (бан)