DMARC

DMARC Domain-based Message Authentication, Reporting and Conformance) — это техническая спецификация, созданная группой организаций для борьбы со спамерами, подделывающими адреса электронной почты отправителей.

Это политика действий с пришедшими письмами, у которых в поле From используется публикующий политику домен. DMARC позволяет не только указать, как поступать с такими письмами, но и собрать статистику от всех получателей, поддерживающих серверную часть DMARC.

http://dmarc.org/

Перед настройкой DMARC нужно настроить SPF и DKIM (Domain Keys Identified Mail)

Параметры

v

Версия протокола (обязательный параметр)

Пример:

```
v=DMARC1
```

p

Правила для домена (обязательный параметр)

- none — не принимать никаких действий
- quarantine — отправлять сообщения в спам
- reject — не принимать сообщения

Пример:

```
p=reject
```

pct

Сообщения, подлежащие фильтрации (в %)

Пример:

```
pct=40
```

ruf

Адрес, на который будут отправляться forensic-отчеты (т. е. исследовательские) по отдельным письмам. По умолчанию forensic-репорты отправляются только по нарушениям DMARC. Можно использовать параметр `fo` для регулирования поведения. В настоящее время относительно небольшое количество получателей отправляет такие отчеты.

Пример:

```
ruf=mailto:ruf@domain.ru
```

rua

Адрес для сводных отчетов.

Пример:

```
rua=mailto:rua@domain.ru
```

sp

Правила для субдоменов

- none — не принимать никаких действий
- quarantine — отправлять сообщения в спам
- reject — не принимать сообщения

Пример:

```
sp=reject
```

fo

По каким нарушениям отправлять уведомления:

- 0 (по умолчанию) — отправлять отчеты, только когда не прошли обе аутентификации: SPF и DKIM.
- 1 — не проходит любая из аутентификация, даже если проходит альтернативный метод
- s — проблемы с SPF
- d — проблемы с DKIM

Пример:

```
fo=1
```

adkim

Режим проверки соответствия DKIM:

- r (relaxed) (по умолчанию)и должен совпадать только организационный домен
- s — строгий режим, требуется полное совпадение домена из адреса отправителя с доменом из DKIM-сигнатуры. Имеет смысл использовать строгое соответствие домена, если часть ваших поддоменов делегирована недоверенным сторонам.

Пример:

```
adkim=r
```

aspf

Режим проверки соответствия для SPF:

- r (relaxed) — разрешать частичные совпадения, например субдоменов данного домена
- s (strict) — разрешать только полные совпадения

Пример:

```
aspf=s
```

ri

Желательный интервал получения аггрегированных отчетов (в секундах). По умолчанию отчеты отправляются раз в сутки (`ri=86400`), но некоторые получатели (не все, т.к. поддержка данного параметра сервером не является обязательной) поддерживают отправку отчетов с более короткими интервалами. На этапе внедрения политики можно попробовать использовать небльшие значения параметра.

Пример:

```
ri=3600
```

DNS

Для почтового домена нужно создать запись DNS:

Имя записи	`_dmarc`
Тип записи	`TXT`
Значение	`v=DMARC1; p=reject; aspf=r; adkim=r; sp=none; pct=100; fo=s; rua=mailto:rua@domain.ru; ruf=mailto:ruf@domain.ru`

Пример готовой записи:

```
_dmarc TXT v=DMARC1; p=reject; aspf=r; adkim=r; sp=none; pct=100; fo=s; rua=mailto:rua@domain.ru;
ruf=mailto:ruf@domain.ru
```

Проверка

DMARC Check Tool - Domain Message Authentication Reporting & Conformance Lookup - MxToolBox

Dmarcian - Protect Your Email and Domain with DMARC

Удобный удобный бесплатный инструмент XML-To-Human Converter для просмотра DMARC-отчетов:
DMARC XML to Human Converter

Просмотр отчётов

dmarc-cat

dmarc-cat

Установка:

```
apt install dmarc-cat
```

Использование:

```
dmarc-cat report.xml
```

или

```
dmarc-cat report.xml.gz
```

Ссылки

Логотип

W DMARC

Настройка DMARC — Помощь Mail.ru. Для разработчиков

HowTo: DMARC / Хабр

Внедрение DMARC для защиты корпоративного домена от спуфинга / Блог компании Mail.ru Group / Хабр

Как прописать DMARC: путеводитель с примерами | Блог UniSender

http://sysadminmosaic.ru/dmarc/dmarc

2020-08-18 20:32