ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Рекомендации по настройке механизмов безопасности почтового сервера, созданного с использованием программного обеспечения с открытым исходным кодом Postfix, от атак, связанных с подменой отправителя (спуфинг-атак)

2025

1. Настройка механизма SPF

1.1 Для проверки SPF-записи для входящей почты в Postfix рекомендуется использовать Postfix Policyd-SPF.

Для установки Postfix Policyd-SPF необходимо выполнить следующие команды в терминале (командной строке) операционной системы (далее по тексту все команды аналогично выполняются в терминале (командной строке) операционной системы):

Для Debian (Ubuntu, Astra Linux):

sudo apt update

sudo apt install postfix-policyd-spf-python

Для CentOS (RHEL):

sudo yum install epel-release

sudo yum install postfix-policyd-spf-python

1.2 После установки необходимо осуществить следующую настройку конфигурации Postfix:

открыть конфигурационный файл Postfix командой *sudo nano /etc/postfix/main.cf;*

добавить в конец файла строку:

policy-spf_time_limit = 3600;

сохранить изменения путем нажатия сочетания клавиш Ctrl+O;

закрыть редактор путем нажатия сочетания клавиш Ctrl+X;

открыть файл /etc/postfix/master.cf командой *sudo nano /etc/postfix/master.cf;*

добавить в конец следующую команду:

policyd-spf unix - n n - 0 spawn

user=policyd-spf argv=/usr/bin/policyd-spf

1.3 Для того, чтобы включить проверку SPF-записи необходимо осуществить следующую настройку конфигурации Postfix:

открыть файл /etc/postfix/main.cf командой *sudo nano /etc/postfix/main.cf;*

найти строку smtpd_recipient_restrictions и добавить check_policy_service unix:private/policyd-spf перед permit следующим образом:

smtpd_recipient_restrictions =

reject_unauth_destination,

check_policy_service unix:private/policyd-spf,

permit

сохранить изменения путем нажатия сочетания клавиш Ctrl+O;

закрыть редактор путем нажатия сочетания клавиш Ctrl+X;

перезапустить сервис Postfix после внесения изменений и применить их командой *sudo systemctl restart postfix* или *sudo service postfix restart.*

1.4 Для проверки настройки SPF-записи необходимо:

отправить тестовое письмо с любого почтового адреса на ваш сервер Postfix;

проверить заголовки командой *sudo tail -f /var/log/mail.log.*

В случае, если SPF настроен правильно, то в логах появится запись *SPF check: pass*. В случае, если письмо не проходит проверку SPF, то в логах появится запись *SPF check: fail.*

2. Настройка механизма DKIM

2.1 Для настройки DKIM в Postfix необходимо установить пакет OpenDKIM путем выполнения команд:

для Debian (Ubuntu, Astra Linux):

sudo apt update

sudo apt install opendkim opendkim-tools -y

для CentOS (RHEL):

sudo yum install epel-release -y;

sudo yum install opendkim opendkim-tools -y.

2.2 После установки необходимо осуществить следующую настройку OpenDKIM:

создать директории для хранения ключей DKIM командами:

sudo mkdir -p /etc/opendkim/keys

sudo chown -R opendkim:opendkim /etc/opendkim

sudo chmod -R 700 /etc/opendkim/keys

создать подпапку для вашего домена (в примере заменить example.ru на ваш реальный домен):

sudo mkdir -p /etc/opendkim/keys/example.ru

сгенерировать DKIM-ключи командой:

sudo opendkim-genkey -b 2048 -d example.com -D /etc/opendkim/keys/example.com -s selector1 -v

Расшифровка параметров:

-b 2048 — длина ключа (рекомендуется 2048 бит);

-d example.ru — ваш домен;

-D /etc/opendkim/keys/example.ru — папка для ключей;

-s selector1 — селектор (можно задать другое имя);

-v — включение режима отладки.

После выполнения команды появятся два файла:

selector1.private — закрытый ключ (используется на сервере);

selector1.txt — публичный ключ (для DNS).

2.3 Необходимо открыть основной конфигурационный файл /etc/opendkim.conf командой:

sudo nano /etc/opendkim.conf;

Добавить или заменить в файле строки следующим образом (в примере директории и порты заменить на реальные данные почтового сервера):

AutoRestart Yes

AutoRestartRate 10/1h

Syslog Yes

LogWhy Yes

Canonicalization relaxed/simple

Mode sv

SignatureAlgorithm rsa-sha256

KeyTable /etc/opendkim/keytable

SigningTable /etc/opendkim/signingtable

TrustedHosts /etc/opendkim/trustedhosts

Socket inet:8891@localhost

2.4 Необходимо настроить таблицы ключей DKIM путем выполнения следующих действий.

Создать файл KeyTable командой:

sudo nano /etc/opendkim/keytable;

добавить в открытый файл строку и сохранить:

selector1._domainkey.example.ru

example.ru:selector1:/etc/opendkim/keys/example.com/selector1.private

Где:

selector1._domainkey.example.ru — DKIM-селектор.

example.ru — ваш домен.

selector1.private — путь к закрытому ключу.

2.5 Осуществить настройку таблицы подписываемых доменов путем создания файла SigningTable командой:

sudo nano /etc/opendkim/signingtable;

и добавлением в созданный файл строки:

**@example.ru selector1._domainkey.example.ru;*

В таком случае все письма с домена example.ru будут подписаны селектором selector1.

2.6 Осуществить настройку доверенных хостов путем создания файла TrustedHosts командой:

sudo nano /etc/opendkim/trustedhosts;

И добавлением строк, содержащих адреса доверенных хостов, например:

127.0.0.1

localhost

example.ru

В случае, если сервер использует внутреннюю сеть, необходимо добавить диапазон IP-адресов следующим образом:

192.168.1.0/24.

2.7 Реализовать настройку Postfix для работы с OpenDKIM следующим образом:

открыть файл /etc/postfix/main.cf командой:

sudo nano /etc/postfix/main.cf;

добавить в конец строки (в примере порты заменить на реальные данные почтового сервера):

 # Подключение OpenDKIM

milter_protocol = 6

milter_default_action = accept

smtpd_milters = inet:localhost:8891

non_smtpd_milters = inet:localhost:8891.

После необходимо перезапустить Postfix командой:

sudo systemctl restart postfix;

2.8 Необходимо добавить DKIM-записи в DNS для этого открыть созданный ранее файл selector1.txt командой:

cat /etc/opendkim/keys/example.com/selector1.txt

В файле будет строка вида:

selector1._domainkey IN TXT ("v=DKIM1; k=rsa; p=MIIBIjANBgkqh...");

скопировать значение публичного ключа *p=MIIBIjANBgkqh…* для добавления его значения в DNS -запись (смотреть пункт 2.3).

2.9 После добавления DNS-записи необходимо перезапустить OpenDKIM следующими командами:

sudo systemctl restart opendkim или *sudo systemctl enable opendkim;*

2.10 Проверка работы OpenDKIM осуществляется командой:

sudo systemctl status opendkim

В случае, если в выводе терминала (командной строки) появилась строка *"Active: active (running)"*, значит сервис работает.

Для проверка слушающего порта необходимо выполнить команду:

netstat -an | grep 8891

Ожидаемый вывод терминала (командной строки):

tcp 0 0 127.0.0.1:8891 0.0.0.0: LISTEN*

3. Настройка механизма DMARC

3.1 Перед настройкой DMARC в Postfix необходимо убедиться, что SPF, DKIM и DMARC записи размещены в DNS (разделы 1-3).

3.2 Для осуществления настройки DMARC в Postfix необходимо установить OpenDMARC командами:

для Debian (Ubuntu, Astra Linux):

apt update && apt install opendmarc

для CentOS (RHEL):

yum install epel-release

yum install opendmarc

Для настройки OpenDMARC необходимо осуществить следующую настройку конфигурации:

открыть конфигурационный файл OpenDMARC командой:

nano /etc/opendmarc.conf;

настроить следующие параметры (в примере директории, IP-адрес и порт заменить на реальные данные почтового сервера):

AuthservID mail.example.ru

PidFile /var/run/opendmarc.pid

UMask 0002

RejectFailures false

Syslog true

TrustedAuthservIDs mail.example.com

IgnoreAuthenticatedClients true

SPFIgnoreResults false

Socket inet:8893@127.0.0.1;

сохранить изменения путем нажатия сочетания клавиш Ctrl+O и закрыть редактор путем нажатия сочетания клавиш Ctrl+X;

3.3 Для настройки OpenDMARC в Postfix необходимо осуществить следующую настройку конфигурации:

открыть конфигурацию Postfix командой:

nano /etc/postfix/main.cf;

добавить поддержку DMARC строками (в примере IP-адреса и порты заменить на реальные данные почтового сервера):

smtpd_milters = inet:127.0.0.1:8893

non_smtpd_milters = inet:127.0.0.1:8893

milter_default_action = accept;

перезапустить Postfix и OpenDMARC командами:

systemctl restart opendmarc

systemctl restart postfix.

Осуществить проверку работоспособности DMARC путем отправки тестового письма с использованием почтового сервера и просмотра заголовков письма (View Message Headers). В случае, если строка *Authentication-Results: dmarc=pass header.from=example.ru* содержит «pass», значит DMARC работает.