Информация для тех, кто уже использует Centos 8. По-умолчанию, на уровне системы отключена поддержка устаревших протоколов TLS 1.0 и 1.1. Но зачастую они еще много где используются. Отсутствие их поддержки создает некоторые неудобства, но это легко исправить, и я расскажу как.

Лично я столкнулся с этой проблемой на обновленном почтовом сервере, который я настроил на Centos 8. Я предполагал, что может возникнуть такая проблема и подстраховался параметрами postfix.

```
smtpd_tls_security_level = may
smtpd_tls_mandatory_protocols = !SSLv2,!SSLv3
smtpd_tls_protocols = !SSLv2,!SSLv3
smtpd_tls_ciphers = low
```

Ожидал, что это позволит подключаться клиентам со старыми версиями TLS. А тем, кто совсем никак не может, оставил возможность подключаться по нешифрованному соединению. По факту некоторым не помогло. У клиентов были различные ошибки. Чаще всего это те, у кого сам tls устарел, но при этом запрещены нешифрованные подключения. Вот несколько вариантов ошибок.

```
TLS connect failed: error:1407742E:SSL routines:SSL23_GET_SERVER_HELLO:tlsv1 alert protocol version;
```

```
14969:error:1409442E:SSL routines:SSL3_READ_BYTES:tlsv1 alert protocol version:s3_pkt.c:1092:SSL alert number 70
```

```
warning: TLS library problem: error:1420918C:SSL routines:tls_early_post_process_client_hello:version too
low:ssl/statem/statem_srvr.c:1655:
```

И все в таком духе. Сервер в активной работе. Таких клиентов хоть и не много было, но тем не менее несколько нашлось. Настройки postfix в части разрешенных протоколов tls не работали, так как они запрещены на уровне системы. Подробнее об этом написано в документации Red Hat.

Для того, чтобы разрешить приложениям работать по протоколам TLS v1.0 и 1.1 необходимо выполнить команду на сервере.

```
# update-crypto-policies --set LEGACY
Setting system policy to LEGACY
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
```

После этого надо перезапустить postfix и проверить с какого-нибудь другого сервера подключиться к целевому по протоколу tls 1.0, например вот так.

```
# openssl s_client -starttls smtp -connect mail.site.ru:25 -tls1
```

Если увидите информацию о сертификате, значит все в порядке. Если какие-то ошибки, то разбирайтесь, почему не работает.

Если же вам не повезло настолько, что надо разрешить работу по протоколу ssl3, то я вам сочувствую :) Я не знаю, каким образом это можно сделать на современной системе. Наверное, придется самим собирать openssl из старых исходников и как-то ставить в систему. Задача не простая.

«CCNA Routing and Switching»;
- Студенты могут сдать экзамен и получить вместе с сертификатом OTUS ещё сертификат курса «CCNA Routing and Switching: Scaling Networks»;

Проверьте себя на вступительном тесте и смотрите программу детальнее по .

Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоем распоряжении. Расскажи, как сделать правильно!

Помогла статья? Есть возможность отблагодарить автора