Подробный отчет о выполненной работе по настройке Asterisk с поддержкой TLS

**Цель:** Настроить Asterisk PBX для работы с TLS, обеспечив безопасное соединение по SIP.

**1. Установка и начальная настройка Asterisk**

Установка Asteriskбыла выполнена на виртуальной машине с ОС Linux. После установки служба Asterisk была запущена, и была проверена её работоспособность.

*sudo systemctl status asterisk*

**Asterisk работает корректно, о чём свидетельствует статус "active (running)".**

**2. Проверка открытых портов**

Проверка портов на наличие активных соединений с помощью `netstat` и `ss` показала, что порт 5060 (UDP) используется Asterisk для обычных SIP-соединений.

*sudo netstat -tuln | grep 5060*

*sudo ss -tuln | grep 5060*

**Результат:** Порт 5060 активен, что подтверждает, что Asterisk настроен и слушает этот порт для SIP-трафика.

**3. Создание и установка сертификатов TLS**

1) Генерация сертификатов: С помощью OpenSSL были созданы файлы сертификатов и закрытых ключей (`denis.crt`, `denis.key`) для TLS-соединений:

*openssl pkey -in /home/denis/denis.pem -out /home/denis/denis.key*

*openssl x509 -in /home/denis/denis.pem -out /home/denis/denis.crt*

*cp /home/denis/denis.crt /home/denis/denis\_cert.pem*

*cp /home/denis/denis.key /home/denis/denis\_key.pem*

2) Установка сертификатов: Файлы сертификатов и ключей были скопированы в соответствующие места и настроены в конфигурационных файлах Asterisk (`sip.conf` и `pjsip.conf`).

**4. Настройка конфигурационных файлов Asterisk**

Настройка `sip.conf`: Включение TLS и настройка соответствующих параметров, таких как путь к сертификатам, разрешённые протоколы и параметры безопасности.

*```ini*

*[general]*

*tlsenable=yes*

*tlsbindaddr=0.0.0.0:5061*

*tlscertfile=/home/denis/denis.crt*

*tlsprivatekey=/home/denis/denis.key*

*tlsdontverifyserver=yes*

Настройка `pjsip.conf`: Создание транспортных настроек для использования TLS на порту 5061, а также настройка конечных точек (endpoints), аутентификации и параметров соединения.

```ini

[tls-transport]

type=transport

protocol=tls

bind=0.0.0.0:5061

tls\_cert\_file=/home/denis/denis\_cert.pem

tls\_priv\_key\_file=/home/denis/denis\_key.pem

**5.** **Перезапуск и проверка работы Asterisk**

1. Перезапуск службы Asterisk после изменения конфигурационных файлов.

*sudo systemctl restart asterisk*

1. Проверка портов после перезапуска:

*sudo ss -tuln | grep 5061*

**Результат:** Порт 5061 теперь слушается для TLS-соединений, подтверждая успешную настройку.

**6. Математическое обоснование выбора портов и безопасности**

1. Порты 5060 и 5061 традиционно используются для SIP и SIP/TLS соответственно. Выбор этих портов обоснован стандартами RFC 3261 (для SIP) и обеспечением безопасности передачи данных через шифрованное соединение TLS на порту 5061.

2) TLS (Transport Layer Security) обеспечивает шифрование данных, передаваемых по сети, защищая SIP-сообщения от прослушивания и атак. Использование TLS с сертификатами гарантирует подлинность сервера и защищает соединение от атак типа «человек посередине».

**7. Заключение**

В результате выполнения всех вышеуказанных шагов, Asterisk PBX был успешно настроен для работы с TLS. Проверка активных портов подтвердила, что сервер слушает как порт 5060 (для обычных SIP-соединений), так и порт 5061 (для защищённых TLS-соединений). Настройка была выполнена корректно, что позволяет использовать Asterisk для безопасных VoIP-коммуникаций.