Система шифрования пакетов

Общее описание

В версии 3.0 системы синхронизации добавилась возможность шифровать и/или подписывать исходящие пакеты. Для этого используется система шифрования GnuPG 1.x, которая поставляется отдельно от системы синхронизации.

Чтобы воспользоваться возможностью шифрования, на обеих сторонах должна стоять система синхронизации версии не ниже 3.0.

По-умолчанию, сразу после установки системы синхронизации версии 3.0, пакеты не шифруются и не подписываются и создаваемые пакеты полностью совместимы с версией 2.x системы синхронизации.

Зашифрованный и/или подписанный пакет внешне выглядит как обычный пакет (`pkt-00000.tgz`), но имеет отличную от версии 2.x структуру. За деталями см. файл `doc/readme.txt` из дистрибутива системы.

В защищенной сети каждый узел должен обладать своей парой ключей, состоящей из открытого и закрытого ключа. Чтобы начать обмениваться с удаленным узлом зашифрованными и/или подписанными пакетами необходимо обменяться с ним открытыми ключами.

Настройка

Для включения шифрования и подписи пакетов необходимо:

1. В конфигурационном файле системы (`etc/sync.conf`) указать путь к каталогу, где будут храниться ключи системы (параметр `SECURITY_HOMEDIR`). Обычно это `/home/sync/etc/keys`.
2. Создать первичную пару ключей, состоящую из открытого и закрытого ключа (команда `syncctl keyring make`).
3. В специальном конфигурационном файле (`etc/nodes.sec`) для каждого узла указать:
   a. уровень безопасности пакетов, формируемых для данного узла:
      0 – пакеты не подписываются и не шифруются
      1 – пакеты подписываются
      2 – пакеты подписываются и шифруются
   b. минимально допустимый уровень безопасности пакетов, приходящих с данного узла:
      0 – пакеты могут не иметь защиты
      1 – пакеты должны иметь хотя бы подпись
      2 – пакеты должны иметь и подпись, и зашифрованные данные
4. Обменяться открытыми ключами с противоположной стороной или, как вариант, создать для удаленной стороны свою пару ключей и установить ее на удаленной стороне как первичную:

Обмен открытыми ключами (например, между оперцентрами)	**Создание пары ключей** (например, в офисе для АЗС)

1. Выгрузить свой открытый ключ в файл `<имя узла>.key`:
`syncctl keyring export`
2. Обменяться ключами каким-либо надежным способом.
3. Добавить открытый ключ противоположной стороны в свое кольцо доверия:
`syncctl keyring add <имя узла>.key`
	1. Создать пару ключей для узла:
	`syncctl keyring make for <узел>`
	2. Скопировать созданную пару ключей (файлы `pubring.gpg` и `secring.gpg`) из каталога
	`/home/sync/etc/keys/<узел>`
	в каталог
	`/home/sync/etc/keys`
	на удаленной системе.