Памятка по безопасности Астериск.

После установки и предварительной настройки Астериска, не спешите выпускать его наружу. Откройте CLI Asterisk набрав '***asterisk -r*** '. Наберите команду '***sip show settings***', это даст возможность увидеть правильно ли Астериск понял, что вы написали в основных конфигах. Первоначально обращаем внимание в секции **Global Settings** на параметры :

AutoCreate Peer: No
Allow unknown access: No
Always auth rejects: Yes

Это как температура больного, дает основные показатели :)
Если не так и просто для очистки совести смотри параметры в sip.conf секция [general]

Жестко запрещаем сусликам-партизанам гостевые звонки. Некоторые SIP-устройства (такие, как Cisco Call Manager v4.1) не поддерживают аутентификацию, поэтому они не смогут устанавливать соединения, если задано allowguest=no. Но оставлять гостевой доступ опасно.
allowguest = no

Далее параметр Autocreatepeer. Он позволяет, если установлен в значение Yes, любым SIP клиентам зарегистрироваться на Вашем сервере Asterisk в качестве пира. Настройки для этого клиента будут установлены из глобальной секции файла конфигурации. Имя пира будет определено, исходя из пользовательской части URL заголовка "Contact:". Эта возможность, если включена, создает большую проблему с безопасностью Вашего сервера, если Вы не контролируете доступ к нему другими средствами (жесткий файрволл).
autocreatepeer = no

Обязательно прописываем свои домены и внешний адрес. При этом запрещаем автосоздание доменов. Если этого не делать, то Asterisk будет добавлять имя локального хоста и локальные IP-адреса в список доменов и считать эти домены обслуживаемыми.
domain = <внутренний IP>, <Внешний IP>
externip = <Внешний IP>
autodomain = no

Жестко укажите локальные сети с которых возможен доступ и те сети которые являются локальными для Астериска. Это позволит работать без проблем с сетями завязанными VPN-туннелями. Так же избавит от проникновения со стороны «домашних» провайдерских сетей. Пример :
Сети которые Астериск считает локальными :
localnet = 192.168.41.0/255.255.255.0
localnet = 192.168.11.0/255.255.255.0
localnet = 192.168.10.0/255.255.255.0
localnet = 192.168.12.0/255.255.255.0

Разрешить регистрацию по умолчанию только из той сети где живет Астериск
Deny = 0.0.0.0/0.0.0.0
Permit = 192.168.41.0/255.255.255.0

Остальным в секциях прописывать конкретную сеть, где они живут :
[1099]
fullname = pupkin-ne-suslik
...
Deny = 0.0.0.0/0.0.0.0
Permit = 192.168.12.0/255.255.255.0

Соответственно пользователь pupkin-ne-suslik, сможет зарегистрироваться только из сети 192.168.12.0. Если даже по кто-то и украл или подсмотрел пароль, то он не войдет снаружи или из другой подсети компании.

Также рекомендую к установке что-то для начала вроде fail2ban. Результат — Суслики попадают в капкан. Штуки по 4 в час.

С Уважением
Блинов Владимир
«РФ-Информатика»
http://it-mehanika.ru
http://rf-informatika.ru
моб. (903)667-23-33
офис (499)502-84-93