Как завести абонента в sip.conf ?

Глобальные настройки [general].  
Данные настройки можно завести 1 раз и не прописывать каждый раз  
под каждым номером, типа [1001], [1002] и т.д.

[general]

***# Базовые настройки.***

context = **outgoing** ; контекст по умолчанию для всех ИСХОДЯЩИХ вызовов от абонентов.

*По умолчанию, он может называться default, но мы перепишем его на outgoing (исходящие).*

*Context в транках для провайдеров будет другой, его мы назовём incoming (входящие).*

*Почему именно так?*

*Таким образом, мы получаем разделение контекста и лучшую безопасность для нашего Астериска.*

*Если свалить всё в кучу, то мы получим нарушение логики маршрутизации. Будет ли работать при  
неправильных настройках? Будет. Но, в результате, мошенник сможет звонить через наш транк  
за наш же счёт!*

***Легкость отладки*** *– любой администратор сразу поймет архитектуру:*

*Входящие звонки – [incoming]*

*Исходящие от абонентов – [outgoing]*

***Если добавится ещё один провайдер SIP-телефонии (IP-телефонии):***

*[general]*

*context = outgoing*

*[zadarma]*

*context = incoming*

*[beeline] ; второй провайдер*

*context = incoming ; Тот же самый контекст для входящих!*

*[megafon] ; третий провайдер*

*context = incoming ; Всё тот же самый контекст для входящих!*

allowguest = no; никаких гостей, мы никого не ждём

allowoverlap = no; разрешить или нет передачу вызова с дополнительными цифрами. Мы говорим НЕТ.

alwaysauthreject = yes; все ошибки для внешнего клиента выглядят одинаково – ошибка авторизации.  
*Эта строка призвана осложнить взлом АТС.*

udpbindaddr = 0.0.0.0:5060 ; принимать звонки на всех адресах этого сервера

bindaddr = 0.0.0.0

bindport = 5060 ; эти две по сути тоже самое, что и udpbindaddr, можно прописывать, можно нет

tcpenable = no ; tcp для SIP-трафика.   
*Некоторые провайдеры, например, Мегафон, требуют, чтобы tcp был включён.*  
*Этот момент нужно уточнить у провайдера.*

language = ru ; язык системы для голосового меню - русский

dtmfmode = rfc2833 ; способ передачи DTMF-сигналов (нажатия клавиш)

*RFC2833 передаёт тоны как RTP-пакеты (самый надёжный способ)*

relaxdtmf = yes ; ослабляет проверку DTMF-пакетов для лучшей совместимости.

*Некоторые телефоны отправляют DTMF с небольшими отклонениями от стандарта.*

rtptimeout = 60; сколько времени клиент может не откликаться, прежде чем будет кикнут из системы

canreinvite = no ; **no** – клиенты общаются через сервер, **yes** – напрямую друг с другом.  
*Запрет перенаправления медиа-потоками (RTP) между абонентами.*

*Из плюсов: безопасность, возможность записи разговоров, учёт детализации, проигрывание голосовых приветствий.*

*В большинстве случаев, всегда ставим no*

***# Настройка кодеков. Можно включать все прописанные ниже и именно в таком порядке.***

allow = ulaw ; отличное качество, похоже на стационарный телефон. Самый поддерживаемый везде.

allow = alaw ; почти тоже самое, что предыдущий. Второй по поддержке.

allow = opus ; современный бесплатный HD-кодек.

allow = g722 ; тоже HD-кодек. HD-голос для современных IP-телефонов и конференций.

allow = g726; устаревший кодек, но широко поддерживается. Для старых телефонов, короч.

allow = gsm ; для мобильных сетей, бесплатный, не требует лицензии. Среднее качество звука.

disallow = all ; выключаем все остальные кодеки.

***# Настройки NAT (критически важные).***

***Если NAT-a нет, это можно не прописывать, или закомментировать.***

localnet = 192.168.1.0/255.255.255.0 ; указываем свою локальную сеть

externip = 95.123.456.789 ; указываем внешний адрес сервера

srvlookup = yes ; включает поиск SRV-записей в DNS для SIP-серверов

allowexternaldomains = yes (no!)

*Данная опция может быть опасна, так как разрешает обработку SIP-запросов для других доменов.  
Обычно это не нужно и здесь ставят* ***no.***

domain = mydomain.com,default

fromdomain = mydomain.com

*Читаем <a href="http://www.voip-info.org/wiki/view/Asterisk+config+sip.conf">тут</a>*

*и решаем надо оно нам, или нет.*

***# Настройки регистрации для транков к провайдерам (эти штуки должны быть внутри general).***

registertimeout = 20 ; ждать ответа от провайдера не более 20 сек.

registerattempts = 0 ; количество попыток регистрации (0 = бесконечно)

*Эти две обычно размещают в секции с транком провайдера, например, в [zadarma], которая идёт прямо под [general], хотя можно и так. Просто некоторые провайдеры крайне привередливы в этим двум опциям.*

defaultexpiry = 3600 ; интервал перерегистрации клиентов (3600 секунд = 1 час)

*Зачем это нужно? Провайдеры периодически требуют перерегистрации.*

minexpiry = 60 ; минимальное допустимое время жизни регистрации = 60 сек.

maxexpiry = 7200 ; максимальное время жизни регистрации = 2 часа.

***# Шифрование и безопасность (примеры настроек).***

1. ***Полное шифрование.***

***Корпоративный вариант. Полное шифрование всего.***

encryption = yes

transport = tls

avpf = yes ; улучшенное шифрование медиа

1. ***Только шифрование медиа (SRTP).***

***Бизнес-вариант. Шифрование голоса, SIP трафик в открытом виде.***

encryption = sdes

transport = udp

1. ***Транспортное шифрование (TLS).***

***Для домашнего использования, т.к. нет конфиденциальных данных.***

encryption = no

transport = tls

НИЖЕ ПРИВЕДЕНЫ ВАРИАНТЫ НАСТРОЕК ДЛЯ АБОНЕНТОВ.

Самый распространённый вариант.

[1001]

type = friend

username = 1001

secret = здесь вводим наш суперсикрет

host = dynamic ; автоматически получать ip от клиента

context = outgoing (это исходящие звонки от внутренних абонентов)

qualify = yes ; время от времени проверять жив абонент, или нет.

qualifyfreq = 60 ; как часто проверять жив ли абонент. Обычно ставят 60 сек.

nat = force\_rport,comedia (если используется NAT) / no (если не используется)

directmedia = no ; если софтфоны за NAT – ставим **NO**, если без NAT – ставим **YES.**

*Определяет, будут ли медиа потоки идти напрямую между телефонами, или через Астериск.*

callerid = “Иван Петров” <1001> (можно только номер, если люди часто меняются)

mailbox = 1001@default

Для софтфонов за NAT.

[1001]

type = friend

username = 1001

secret = наш пароль

host = dynamic

context = outgoing

nat = force\_rport,comedia (за NAT) / no (без NAT)

directmedia = no (за NAT) / yes (без NAT)

qualify = yes

qualifyfreq = 60

Для физического SIP-телефона в локальной сети.

[1001]

type = friend

username = 1001

secret = наш суперсикрет

host = 192.168.1.100 ; здесь нужно указывать фиксированный IP телефона

context = outgoing

directmedia = yes

qualify = yes

qualifyfreq = 60

По шаблону.

*Самый интересный вариант. Клиентов, как правило, довольно много, поэтому, чтобы не прописывать каждому одно и тоже, мы используем шаблоны. Выглядит это так.*

*Т.е. сначала в sip.conf загоняется секция [general], внутрь [general] загоняется строчка с register =>, для регистрации транка с провайдером, затем загоняется сама секция с провайдером, например, [zadarma], затем шаблон, например, [friend](!), а затем пользюки [ext1001](friend), [ext1002](friend) и т.д.*

**[friend](!)**

*Восклицательный знак делает шаблон абстрактным – его нельзя использовать для регистрации телефона, он служит только чертежом для других секций. Без (!) кто-то может случайно зарегистрировать телефон с именем [friend], что создаст уязвимость.*l = autosack68.1.0/255.255.255.0ивередливы в этим двум опциям.

**------** Базовый тип и хост ------

**type = friend**

*Универсальный тип абонентов, можно как принимать, так и совершать вызовы.*

**host = dynamic**

*IP адрес абонента неизвестен, он будет сообщаться в период регистрации. В большинстве случаев прописываем dynamic.*

------ Безопасность ------

**deny = 0.0.0.0/0.0.0.0**

**permit = 192.168.1.0/255.255.255.0**

*Создаём белый список IP адресов. Сначала запрещаем все (deny = 0.0.0.0/0), а затем разрешаем только адреса  
из сети 192.168.1.0/24. Это критически важная защита. Регистрация и звонки будут приниматься только  
из нашей локальной сети. Любая попытка подключиться из интернета будет блокирована, даже если*

*злоумышленник угадает пароль.*

**acl = autosack**

*Включает механизм Auto-SACK. Астериск автоматически будет добавлять в чёрный список IP адреса, с которых  
поступает много неудачных попыток регистрации. Это защита от брутфорса. После нескольких неудачных  
попыток атакующий будет заблокирован на некоторое время.*

------ NAT и медиа ------

**qualify = yes**

**qualifyfreq = 60**

*Астериск периодически отправляет на телефон SIP-пакет и таким образом проверяет жив ли абонент.*

*Частота проверки телефонов – каждые 60 секунд.*

**nat = здесь либо force\_rport,comedia, либо no**

*force\_rport – заставляет Астериск использовать порт из источника пакета для ответа, что необходимо  
для работы через большинство NAT-устройств.*

*comedia – заставляет Астериск открыть RTP-порт первым, чтобы телефоны за NAT смогли принять медиа-поток.*

*Зачем это нужно? Это для лечения проблемы «я тебя слышу, а ты меня – нет».  
Здесь должно быть либо yes, либо force\_rport,comedia для телефонов в локальной сети.*

**directmedia = no (явный аналог canreinvite = no, на уровне абонента)**

*Запрещает телефонам устанавливать прямой RTP-поток (голос) между собой, минуя Астериск.*

*Если здесь поставить yes, перестанут работать:  
- запись разговоров*

*- учёт трафика (биллинг)*

*- голосовое меню (IVR) и очереди (Queue) при переводе вызова*

*- статистика и мониторинг вызовов*

**rtpkeepalive = 5**

*Раз в 5 секунд Астериск отправляет в RTP-поток специальный «пустой» пакет, чтобы поддерживать открытыми  
порты на NAT-устройстве. Зачем это нужно? Предотвращает преждевременное «засыпание» NAT-сессии во время  
длинных разговоров, что может привести в обрыву звука.*

------ Качество связи и сессии ------

**session-timers = originate**

*Астериск будет сам инициировать механизм обновления SIP-сессии, отправляя пакет UPDATE, или re-INVITE.*

*Помогает обнаружить «зависшие» вызовы, например, если телефон потерял связь.*

**session-expires = 1800**

*Интервал обновления сессии 1800 секунд (30 минут). Определяет, как часто нужно «продлевать» вызов.*

**session-minse = 90**

*Устанавливает минимально допустимый интервал обновления сессии в 90 секунд.*

*Зачем это нужно? Это защита от слишком частых обновлений, которые могут запросить «глючные» телефоны.*

**session-refresher = uas**

*Указывает, что инициатором обновления сессии всегда будет Астериск.  
Зачем это нужно? Централизует управление сессиями на сервере, повышая предсказуемость и стабильность.*

**dtmfmode = rfc2833**

*Указывает телефону использовать метод RFC2833 для передачи нажатий клавиш (DTMF).*

*Это самый надёжный и быстрый способ, который корректно работает через NAT и не искажает звук.*

------ Идентификация и лимиты ------

**call-limit = 1**

*Количество одновременных исходящих вызовов от 1 абонента = 1.  
Эта защита от мошенников. Если пароль скомпрометирован, они не смогут звонить на 10 линий одновременно.*

**busylevel = 1**

*Устанавливает порог «занятости» абонента. Как только у него будет 1 активный вызов, он будет считаться занятым. Зачем это нужно? При достижении лимита все последующие вызовы на этот номер будут получать  
сигнал «занято» или перенаправляться на голосовую почту.*

*Сразу после секции [friend](!) пишем секции с пользюками, делается это так.*

[ext1000](friend)

secret = password12345

callerid = “Иван Петров” <1000>

mailbox = 1000@default ; 🡨 Голосовая почта для абонента 1000, если она есть. Если нет, не указываем.

[ext1001](friend)

secret = password12345

callerid = “Мария Сидорова” <1001>

mailbox = 1001@default ; 🡨 Голосовая почта для абонента 1001, если она есть. Если нет, не указываем.