



FAQ v 1.0
КОМПЛЕКСНАЯ ЗАЩИТА MyPBX

Оглавление

Введение	3
Настройка межсетевого экрана	4
Правило для доступа к внутренним службам IP-АТС	6
Правило доступа к IP-АТС из локальной сети	7
Правило для удаленного доступа к веб-интерфейсу IP-АТС с заданного внешнего IP-адреса	8
Правило для удаленного доступа к IP-АТС по протоколу SSH с заданного внешнего IP-адреса	9
Правило для подключения учетной записи VoIP-оператора	9
Правило «Запретить все»	10
Автоматическая защита	11
SIP-защита	12
Смена паролей установленных по умолчанию	13
Пароль доступа к веб-интерфейсу	13
Пароль доступа к IP-АТС по протоколу SSH	14
Пароль для личного кабинета пользователя (User Web Interface)	15
Пароль доступа к интерфейсу функции записи разговоров	16
Настройка ограничения пользования SIP-номерами по IP-адресам абонентских устройств	17
Настройка ограничения доступа к конкретному SIP-номеру по IP-адресу	18
Настройка ограничения доступа к группе SIP-номеров по IP-адресу	19
Изменение портов установленных по умолчанию для доступа по протоколам HTTP и SSH	21
Изменение порта HTTP для доступа к веб-интерфейсу	21
Изменение порта SSH	22

Введение

IP-АТС является сетевым устройством, которое может подвергаться атакам злоумышленников с целью получения доступа к исходящим каналам. Данный метод компьютерного преступления очень распространен в настоящее время, поэтому во избежание несанкционированного доступа к исходящим каналам связи рекомендуем настроить комплексную защиту IP-АТС:

- Настройка межсетевого экрана IP-АТС.
- Смена паролей установленных по умолчанию.
- Настройка ограничения пользования SIP-номерами по IP-адресам абонентских устройств.
- Изменение портов установленных по умолчанию для доступа по протоколам HTTP и SSH.

Необходимость обеспечить защиту IP-АТС возникает

- при использовании функции подключения удаленных абонентов или других IP-АТС, находящихся во внешней сети (см. FAQ «Подключение удаленных абонентов и сопряжение с другими IP-АТС»).
- при установке IP-АТС на реальный «белый» IP-адрес внешней сети.

Если IP-АТС установлена в локальной сети за маршрутизатором без проброса портов, то в общем случае настраивать защиту необходимости нет, но мы настоятельно рекомендуем сделать это в любом случае и при любом типе подключения.

Настройка межсетевого экрана

Перед началом конфигурирования межсетевого экрана рекомендуется сделать резервную копию Ваших настроек с помощью меню веб-интерфейса IP-АТС в разделе **«Системные настройки»-«Резервное копирование»**

Данное примечание необходимо на тот случай, если при ошибке в настройке межсетевого экрана Вы закроете себе доступ к IP-АТС. Тогда Вы сможете сбросить все настройки, нажав кнопку **«Reset»** на задней панели IP-АТС, и восстановить конфигурацию с помощью файла резервного копирования.

Внимание! Правила по умолчанию, созданные в межсетевом экране в разделе **«Автоматическая блокировка IP-адресов»** имеют наивысший приоритет. Данные правила являются минимальной защитой IP-АТС от перебора паролей и не могут гарантировать защиту на 100%. Для защиты IP-АТС рекомендуется полностью закрыть доступ с помощью чекбокса **«Запретить все»**, но для этого необходимо:

- создать правила со статусом **«Разрешить»** в разделе **«Правила»**
- удалить правила по умолчанию в разделе **«Автоматическая блокировка IP-адресов»**

Удаление правил необходимо для корректной работы новых правил в разделе **«Правила»** межсетевого экрана.

Для настройки межсетевого экрана зайдите на веб-интерфейс IP-АТС в раздел **«Системные настройки»** и выберите вкладку **«Межсетевой экран»**.

настройка ↗

Настройки

Включить межсетевой экран

Примечание:

1. Необходимо перезагрузить систему после изменений.
2. Настоятельно рекомендуется добавить локальный сетевой адрес в белый список, в противном случае он может попасть в черный список.

Межсетевой экран включен

Правила

+ Новое правило

Правила не заданы

Автоматическая защита

+ Новое правило

Правила не заданы

Автоматическая блокировка IP-адресов

+ Новое правило

Список IP-адресов

Порт	Протокол	Интервал	
5060	UDP	120/60s	Редактировать ✕ Удалить
5060	UDP	40/2s	Редактировать ✕ Удалить
8022	TCP	5/60s	Редактировать ✕ Удалить

Правила по умолчанию

Параметр	Описание
Включить межсетевой экран	Включение/Выключение межсетевого экрана. По умолчанию: Включено. Сетевой экран по умолчанию включен, поэтому без настройки особых

	правил в Черном списке могут оказаться и локальные абонентские устройства, проявляющие сетевую активность (например, телефон опрашивающий сеть для функции BLF (отображение статуса абонента)).
Режим невидимости	Устройство не будет отвечать на запросы ICMP (ping).
Запретить все	Система будет отклонять все запросы, если другое не определено правилами.

Для создания правила в меню «**Правила**» нажмите на кнопку «**+Новое правило**».

Параметр	Описание
Имя	Имя правила. Заполняется в свободной форме.
Описание	Описание к правилу. Заполняется в свободной форме.
Протокол	Протокол передачи данных: TCP, UDP или BOTH (оба).
Порт	Диапазон портов для данного правила.
IP	IP-адрес или сеть, для которых применяется данное правило.
MAC	MAC-адрес устройства, для которого применяется данное правило. Указывается, если требуется дополнительное определение устройства по MAC-адресу.
Действие	Заблокировать – заблокировать пакеты. Разрешить – разрешить обработку пакетов. Игнорировать – игнорировать пакеты.

Правило для доступа к внутренним службам IP-АТС

При работе режима «**Запретить все**» необходимо открыть доступ модулю управления (веб-интерфейс) IP-АТС к внутренним службам (изменение конфигурации, мониторинг, запись разговоров и т.д.):

Новое правило

Имя *i*: Доступ к внутренним службам

Описание *i*: 127.0.0.1

Протокол *i*: ВОТН

Порт *i*: 1 : 65535

IP *i*: 127.0.0.1 / 255.255.255.255

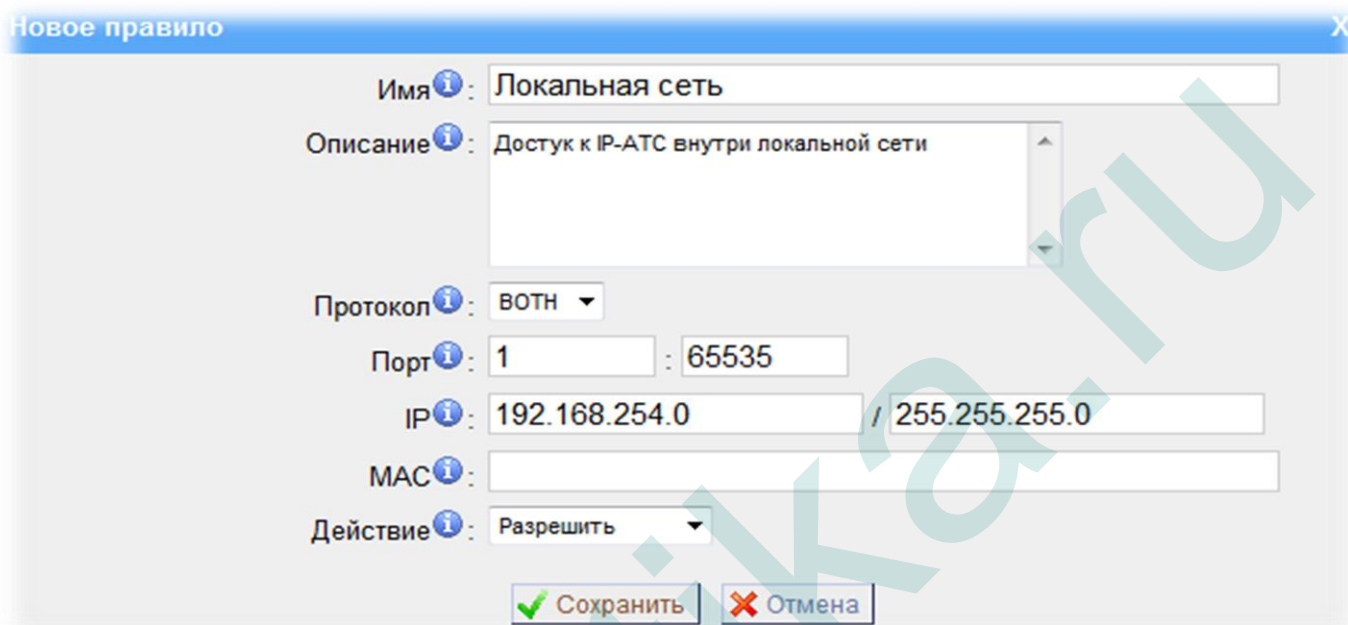
MAC *i*:

Действие *i*: Разрешить

✓ Сохранить ✗ Отмена

Правило доступа к IP-АТС из локальной сети

Правило для работы локальных абонентских устройств с IP-АТС или для доступа к IP-АТС из локальной сети



Новое правило

Имя: Локальная сеть

Описание: Достук к IP-АТС внутри локальной сети

Протокол: ВОТН

Порт: 1 : 65535

IP: 192.168.254.0 / 255.255.255.0

MAC:

Действие: Разрешить

Сохранить Отмена

В примере указан диапазон IP-адресов для доступа к IP-АТС в локальной сети.

192.168.254.0/255.255.255.0 – данный диапазон означает, что любой IP-адрес из локальной сети 192.168.254.x/255.255.255.0, где x – любое число в диапазоне от 0 до 255, имеет доступ к IP-АТС.

Правило для удаленного доступа к веб-интерфейсу IP-АТС с заданного внешнего IP-адреса

Новое правило X

Имя *i*: HTTP

Описание *i*: Удаленный доступ к веб-интерфейсу

Протокол *i*: TCP

Порт *i*: 80 : 80

IP *i*: 210.34.145.101 / 255.255.255.255

MAC *i*:

Действие *i*: Разрешить

Порт 80 – это порт по умолчанию для подключения к IP-АТС по протоколу HTTP. Порт настраивается в веб-интерфейсе IP-АТС в разделе «Системные настройки», меню «Настройки».

Правило для удаленного доступа к IP-АТС по протоколу SSH с заданного внешнего IP-адреса

Новое правило

Имя *i*: SSH

Описание *i*: Удаленный доступ через SSH

Протокол *i*: TCP

Порт *i*: 8022 : 8022

IP *i*: 210.34.145.210 / 255.255.255.255

MAC *i*:

Действие *i*: Разрешить

Сохранить Отмена

Порт 8022 – это порт по умолчанию для подключения к IP-АТС по протоколу SSH. Настраивается в веб-интерфейсе IP-АТС в разделе «Системные настройки», меню «Настройка сети».

Правило для подключения учетной записи VoIP-оператора

Новое правило

Имя *i*: МТТ

Описание *i*: Allow МТТ

Протокол *i*: UDP

Порт *i*: 1024 : 65535

IP *i*: 80.75.130.134 / 255.255.255.255

MAC *i*:


Действие *i*: Разрешить


Сохранить Отмена

Правило «Запретить все»

После создания перечисленных выше правил можно применить правило «**Запретить все**», обезопасив тем самым IP-АТС от несанкционированных подключений.

▶ Дополнительные настройки

 Режим невидимости

 Запретить все

ipmatika.ru

Автоматическая защита

Данные правила представляют собой ограничение по количеству подключений за единицу времени. Для создания правила такого типа необходимо создать правило в опции «**Автоматическая защита**» в меню настройки межсетевого экрана.

Нажмите на кнопку «**+Новое правило**» и введите нужные данные:

Параметр	Описание
Порт	Указывается порт, на который требуется сделать ограничение.
Протокол	Указывается протокол TCP или UDP, для которого будет действовать данное ограничение.
Интервал	Указывается максимальное количество активных соединений за единицу времени. Единицы: Секунда, Минута, Час.

Данное правило означает, что на порту 80 могут быть обработано от 1 до 20 TCP запросов в минуту, 21 запросу будет отказано в доступе.

SIP-защита

Данные правила представляют собой ограничение по количеству SIP-пакетов за единицу времени. Для создания правила такого типа необходимо создать правило в опции «**SIP защита**» в меню настройки межсетевого экрана.

Нажмите на кнопку «**+Новое правило**» и введите нужные данные:

Параметр	Описание
Порт	Указывается порт, на который требуется сделать ограничение.
Протокол	Указывается протокол TCP или UDP, для которого будет действовать данное ограничение.
SIP-пакеты	Количество SIP-пакетов.
Интервал	Интервал времени.

Данное правило означает, что 90 SIP-пакетов будут обработаны IP-АТС за 60 секунд.

или

20 SIP-пакетов будут обработаны за 2 секунды.

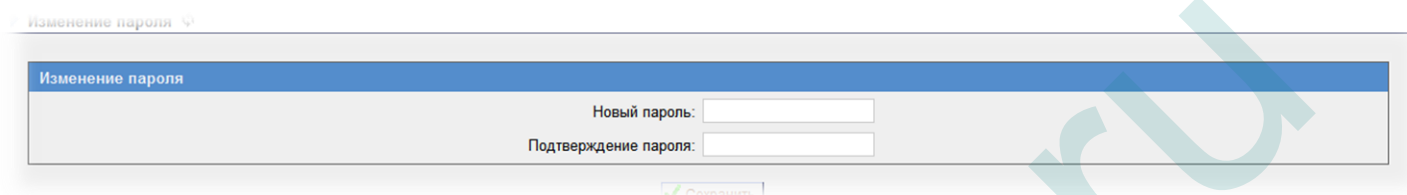
Данные правила существуют по умолчанию и помогают защититься от подбора паролей для доступа к IP-АТС.

Смена паролей установленных по умолчанию

Пароль доступа к веб-интерфейсу

Для изменения пароля веб-интерфейса МуРВХ зайдите:

Веб-Интерфейс МуРВХ - > Дополнительные настройки - > Изменение пароля



The screenshot shows a web browser window with a breadcrumb trail: «Изменение пароля». The main content area has a blue header with the text «Изменение пароля». Below the header, there are two input fields: «Новый пароль:» and «Подтверждение пароля:». At the bottom of the form, there is a button with a green checkmark icon and the text «Сохранить».

Введите пароль, подтвердите ввод пароля (введите еще раз), нажмите кнопку «Сохранить»

Пароль доступа к IP-АТС по протоколу SSH

Для смены пароля SSH необходимо подключиться к IP-АТС с помощью клиента SSH, например putty:

```
192.168.254.231 - PuTTY
login as: root
root@192.168.254.231's password: █
```

```
192.168.254.231 - PuTTY
login as: root
root@192.168.254.231's password:

BusyBox v1.4.1 (2012-04-11 15:35:00 CST) Built-in shell (msh)
Enter 'help' for a list of built-in commands.

root:~> █
```

```
192.168.254.231 - PuTTY
login as: root
root@192.168.254.231's password:

BusyBox v1.4.1 (2012-04-11 15:35:00 CST) Built-in shell (msh)
Enter 'help' for a list of built-in commands.

root:~> passwd root
Enter new Unix password:
Re-enter new Unix password:
root:~> █
```

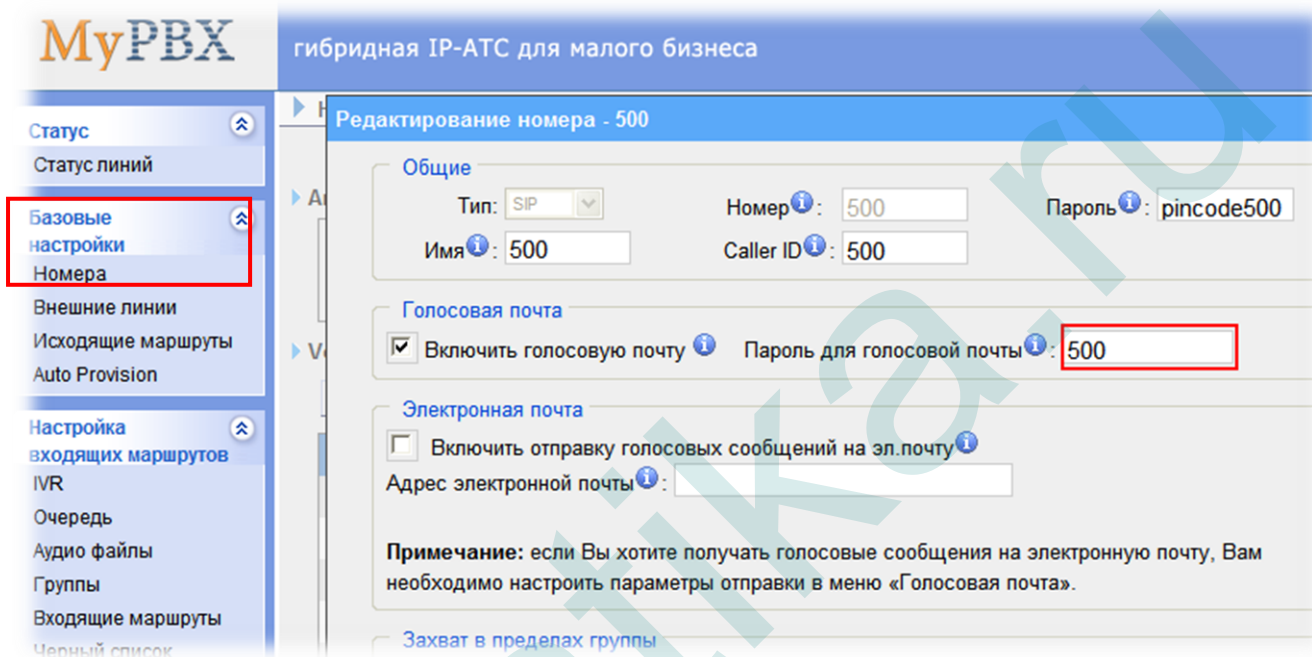
Внимание! Доступ SSH предназначен для мониторинга и выявления проблем. Все настройки МуРВХ необходимо выполнять из веб-интерфейса.

Пароль для личного кабинета пользователя (User Web Interface)

Изменить пароль доступа к личному кабинету пользователя (User Web Interface) можно двумя способами:

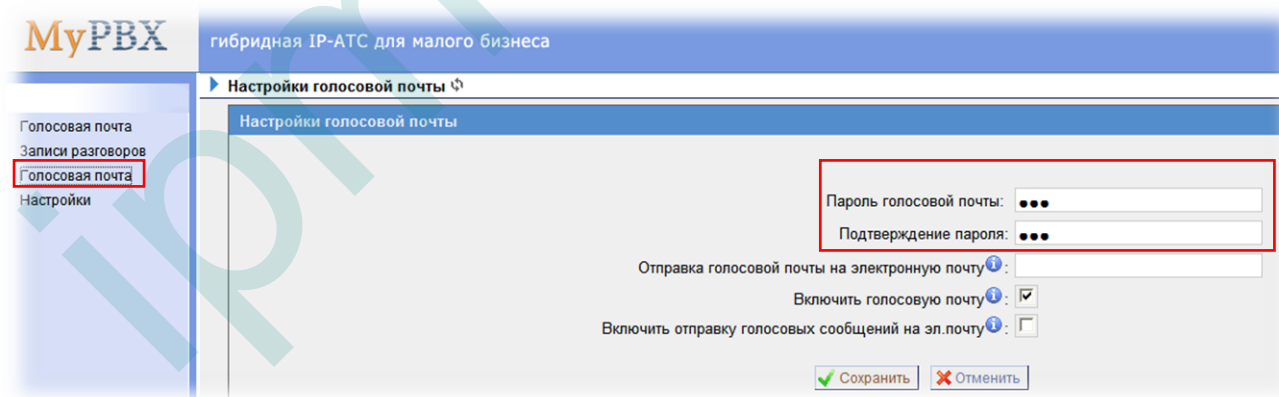
1. Из основного меню веб-интерфейса под учетной записью администратора

Веб-интерфейс - > Базовые настройки - > Номера - > Редактировать номер



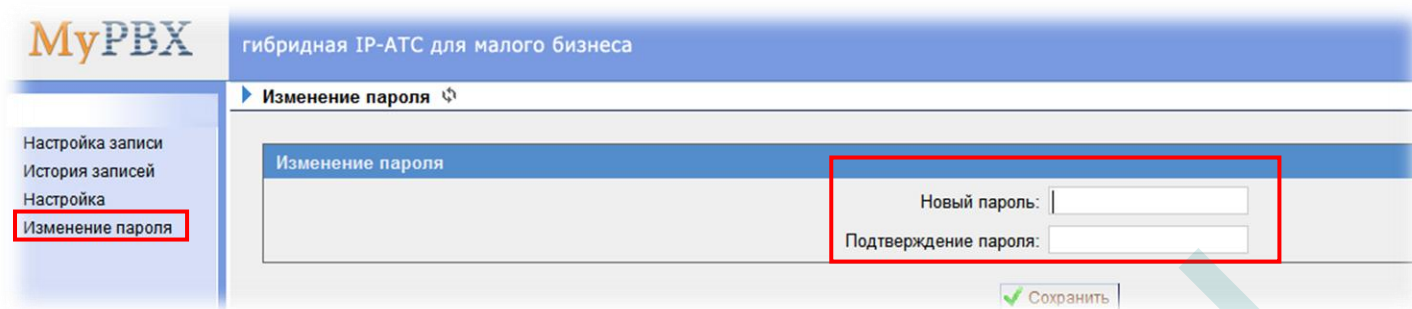
2. Из личного кабинета пользователя (User Web Interface)

Зайдите в личный кабинет пользователя (User Web Interface)



В разделе «Голосовая почта» введите пароль и подтвердите его.

Пароль доступа к интерфейсу функции записи разговоров



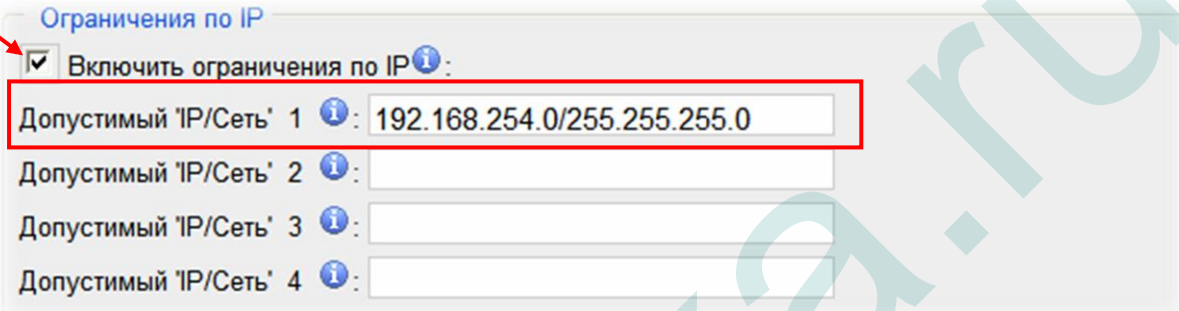
The screenshot shows the MyPBX web interface. The top header includes the MyPBX logo and the text 'гибридная IP-АТС для малого бизнеса'. A left sidebar contains navigation links: 'Настройка записи', 'История записей', 'Настройка', and 'Изменение пароля' (highlighted with a red box). The main content area is titled 'Изменение пароля' and contains two input fields: 'Новый пароль:' and 'Подтверждение пароля:', both highlighted with a red box. A 'Сохранить' button with a green checkmark is located below the fields.

Зайдите в интерфейс функционала записи разговоров используя комбинацию логин/пароль (monitor/password). В разделе «**Изменение пароля**» введите новый пароль и подтвердите его. Нажмите кнопку «Сохранить».

Настройка ограничения пользования SIP-номерами по IP-адресам абонентских устройств

Для ограничения пользования SIP-номерами по IP-адресу абонентского устройства и/или по IP-адресу локальной сети зайдите:

Веб-интерфейс - > **Базовые настройки** - > **Номера** - > **Редактирование номера** - > **Дополнительные настройки** - > **Ограничения по IP**



Ограничения по IP

Включить ограничения по IP *i*:

Допустимый 'IP/Сеть' 1 *i*: 192.168.254.0/255.255.255.0

Допустимый 'IP/Сеть' 2 *i*:

Допустимый 'IP/Сеть' 3 *i*:

Допустимый 'IP/Сеть' 4 *i*:

Для включения функции ограничения пользования SIP-номерами по IP-адресу абонентского устройства и/или по IP-адресу локальной сети поставьте галочку в чекбоксе «**Включить ограничение по IP**». В поле «**Допустимый IP/Сеть**» введите локальный IP-адрес абонентского устройства или IP-адрес вашей локальной сети:

192.168.254.0/255.255.255.0 – Данное правило разрешает регистрацию любому IP-адресу из локальной сети 192.168.254.xxx

192.168.254.27/255.255.255.0 – Данное правило разрешает регистрацию только указанному IP-адресу.

Возможно добавить ограничение как к конкретному номеру так и [к группе номеров](#).

Настройка ограничения доступа к конкретному SIP-номеру по IP-адресу

Настройка функций

- SIP-настройки
- IAX-настройки
- Голосовая почта
- SMS
- DISA
- Конференции
- Оповещение и интерком
- DNIS настройки
- Настройки PIN
- Настройка CallBack
- Быстрый набор
- Музыка в режиме ожидания

Сетевые настройки

- LAN
- WAN
- Маршрутизация
- Межсетевой экран
- DHCP-сервер
- VLAN
- OpenVPN
- DDNS

Дополнительные настройки

- Архив
- Изменение пароля
- Голосовые сообщения
- Дата и время

Показать: 1-25

Всегда

Переадресация: Нет ответа Занято Действие: Голосовая почта Номер 120

Дополнительные функции

Ожидание DND Личный кабинет Время: 8

Контроль разговора

Разрешить контроль Режим:

Дополнительные настройки

VoIP-настройки

NAT: Qualify: SRTP:

Транспорт: UDP Режим DTMF: RFC2833

Ограничения по IP

Включить ограничения по IP

Допустимый 'IP/Сеть' 1: 192.168.254.0/255.255.255.0

Допустимый 'IP/Сеть' 2:

Допустимый 'IP/Сеть' 3:

Допустимый 'IP/Сеть' 4:

Внешний номер

Использовать Номер:

Поддержка T.38

Использовать номер в качестве факса T.38

Сохранить Отменить

Настройка ограничения доступа к группе SIP-номеров по IP-адресу

Для настройки ограничения доступа к SIP-номерам по IP-адресу для группы SIP-номеров необходимо зайти:

- **Веб-интерфейс** - > **Базовые настройки** - > **Номера** ;
- Отметить номера, которые необходимо отредактировать и нажать кнопку **«Редактировать выбранные номера»**

VoIP-номера

<input type="checkbox"/>	Номер	Тип	Имя	Caller ID
<input checked="" type="checkbox"/>	100	SIP		100
<input type="checkbox"/>	101	SIP		101
<input checked="" type="checkbox"/>	102	SIP		102
<input checked="" type="checkbox"/>	103	SIP		103
<input checked="" type="checkbox"/>	104	SIP		104
<input checked="" type="checkbox"/>	105	SIP		105
<input checked="" type="checkbox"/>	106	SIP		106
<input checked="" type="checkbox"/>	107	SIP		107
<input checked="" type="checkbox"/>	108	SIP		108

Появится окно массового редактирования параметров выбранных SIP-номеров:

Статус линий

Базовые настройки
Номера
Внешние линии
Исходящие маршруты
Auto Provision

Настройка входящих маршрутов
IVR
Очередь
Аудио файлы
Группы
Входящие маршруты
Черный список

Системные настройки
Настройки
Режим работы
Настройка функций
SIP-настройки
IAX-настройки
Голосовая почта
SMS
DISA
Конференции
Оповещение и интерком
DNIS настройки
Настройки PIN
Настройка CallBack

Аналоговые
Порт
5

VoIP-номера
+ Добавить

Редактирование выбранных номеров

Общие

Пароль: для всех номеров
 Использовать + номер как пароль
 Разрешить контроль
 Режим:

Голосовая почта

Включить голосовую почту
 Пароль для голосовой почты: для всех номеров
 Использовать номер как PIN
 Адрес электронной почты:

VoIP-настройки

NAT
 Режим DTMF: RFC2833
 SRTP
 Qualify

Ограничения по IP

Включить ограничения по IP
Допустимый 'IP/Сеть' 1 :
Допустимый 'IP/Сеть' 2 :
Допустимый 'IP/Сеть' 3 :
Допустимый 'IP/Сеть' 4 :

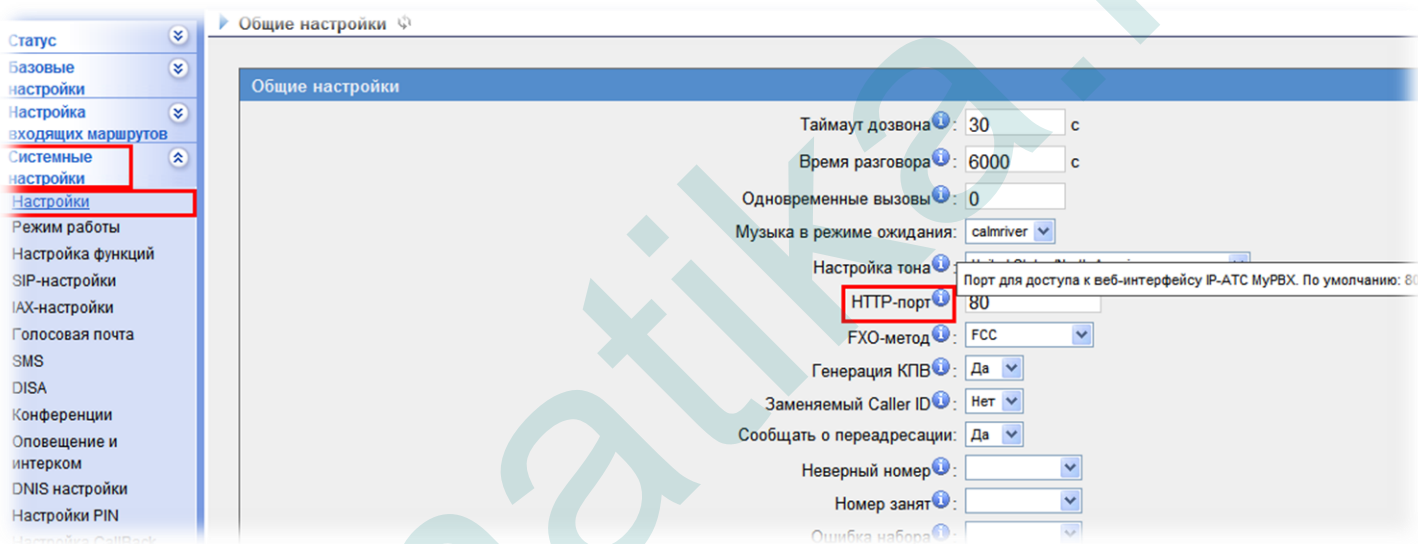
Захват в пределах группы

Изменение портов установленных по умолчанию для доступа по протоколам HTTP и SSH

Изменение порта HTTP для доступа к веб-интерфейсу

Для изменения HTTP-порта по умолчанию для доступа к веб-интерфейсу IP-АТС зайдите:

Веб-интерфейс - > Системные настройки - > Настройки - > HTTP-порт

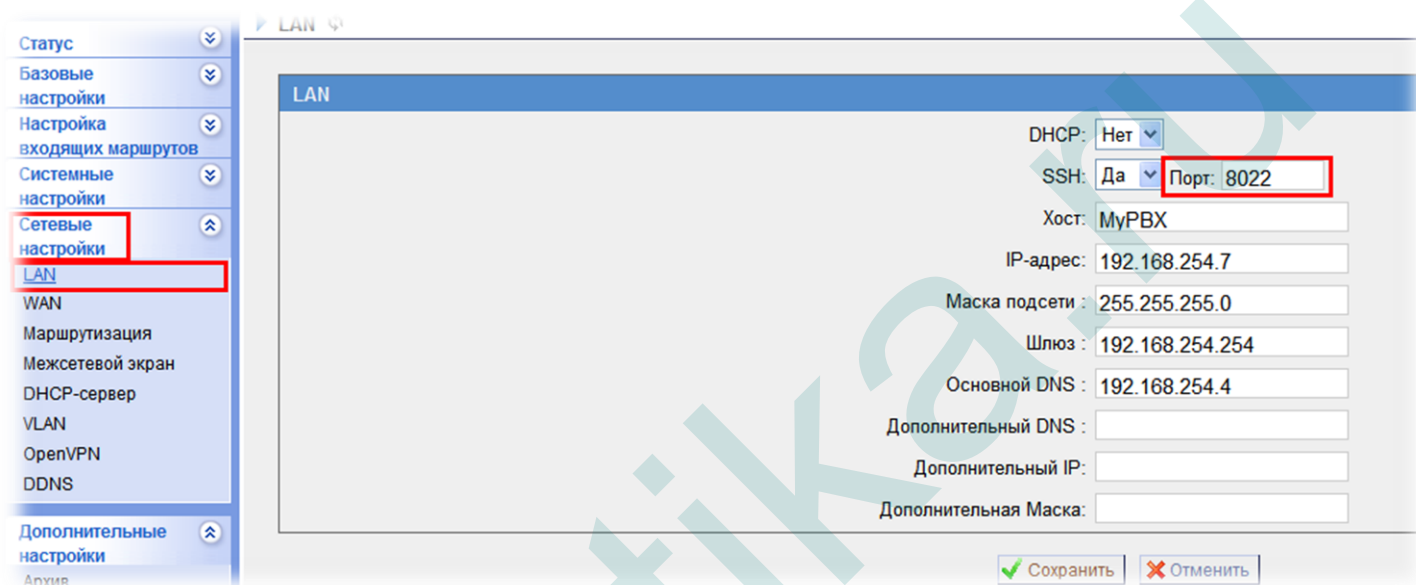


Внимание! После смены HTTP-порта по умолчанию доступ к IP-АТС будет возможен только с указанием не стандартного HTTP-порта (например **8080) и будет иметь вид:**
<http://192.168.5.150:8080/>

Изменение порта SSH

Для изменения порта для доступа к IP-АТС по протоколу SSH необходимо зайти:

Веб-интерфейс - > Сетевые настройки - > LAN



После изменения порта по умолчанию необходимо нажать кнопку «**Сохранить**» и выполнить перезагрузку IP-АТС.