

IT база знаний  
[wiki.merionet.ru](http://wiki.merionet.ru)

# Бесплатный курс по Asterisk

УСТАНОВКА, НАСТРОЙКА, БЕЗОПАСНОСТЬ, ТРАБЛШУТИНГ



МЕРИОН НЕТВОРКС

## Блок 4.

# Безопасность сервера Asterisk

## Обзор

1. [Повышение безопасности Asterisk](#)
2. [Какие порты открыть для Asterisk/FreePBX?](#)
3. [FreePBX - обнаружение слабых паролей](#)
4. [Конфигурация Firewall в FreePBX](#)
5. [Настройка SSL в FreePBX](#)
6. [Лучшие практики по защите SSH подключения](#)
7. [Генератор устойчивых паролей](#)
8. [Домашнее задание.](#)

## Повышение безопасности Asterisk

О том, как защитить IP-АТС от несанкционированного доступа и дадим несколько простых советов, следуя которым, можно существенно повысить безопасность вашей телефонной станции. Примеры, которые будут приведены в данном разделе, относятся к IP-АТС на базе Asterisk, однако многие из них распространяются на все без исключения VoIP-АТС.

Для начала, давайте разберемся, чем же грозят “дыры” в безопасности и какие последствия грозят бизнесу, если злоумышленник получит доступ к IP-АТС.

### Угроза взлома

В отличие от взлома персонального компьютера или почты, взлом АТС – это бесплатные для взломщика звонки, за которые придется заплатить владельцу АТС. Известно немало случаев, когда хакеры тратили колоссальные суммы, проведя на взломанной АТС всего несколько часов.

Как правило, целями злоумышленников становятся IP-АТС, которые доступны из публичной сети. Используя различные SIP-сканнеры и исследуя системные уязвимости, они выбирают места для атаки. Дефолтные (**default**) пароли, открытые SIP-порты, неправильно управляемый **firewall** или его отсутствие - всё это может стать причиной несанкционированного доступа.

К счастью, все эти уязвимости можно устранить и причём совершенно бесплатно.

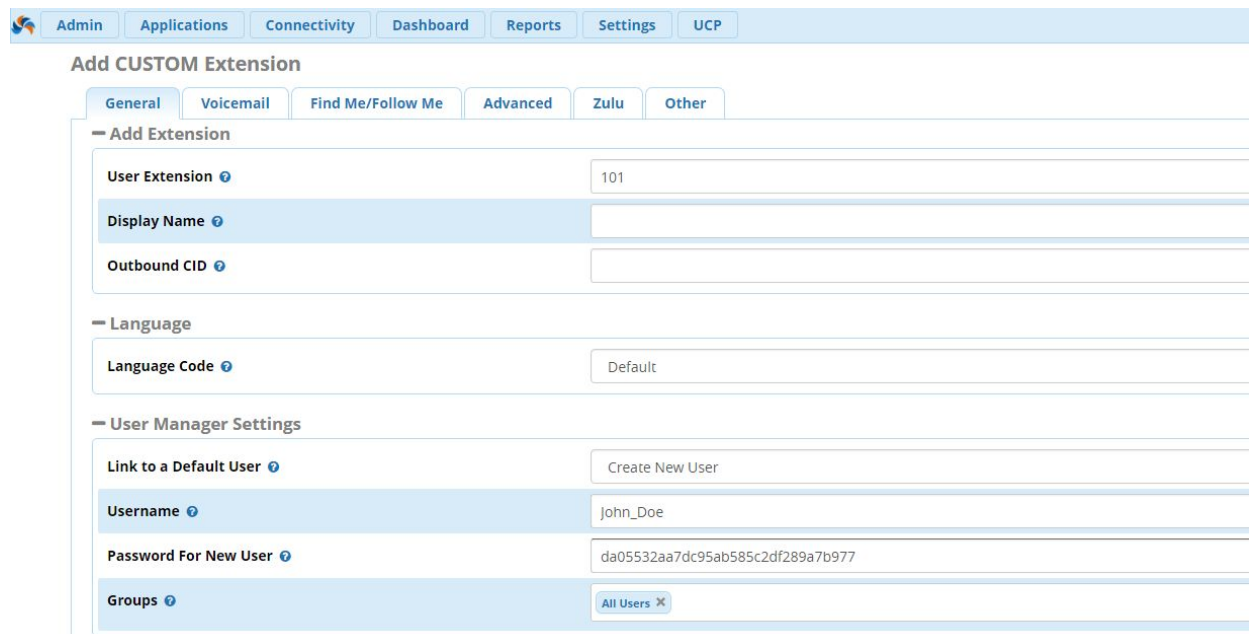
## Простые шаги к повышению безопасности

1. Первое правило, которое необходимо соблюдать – это не афишировать адрес своей IP-АТС и следить за тем, чтобы доступ к сети имели только авторизованные пользователи. Разумеется, это правило распространяется и на физический доступ к серверу, на котором установлена IP-АТС.
2. Второе и самое очевидное – не использовать дефолтные (default) пароли, которые будет легко подобрать или угадать – “1234”, “admin”, “password”, название компании и так далее.

Одной из самых распространённых ошибок, является создание внутренних номеров (Extension), у которых и номер и пароль совпадают. В **sip.conf** это выглядит примерно так:

```
sip.conf
[101]
username=101
secret=101
host=dynamic
```

Допускать такого, категорически нельзя. Тем более что при создании внутреннего номера через интерфейс FreePBX, автоматически генерируется 32-значный надёжный пароль.



The screenshot shows the 'Add CUSTOM Extension' page in the FreePBX web interface. The top navigation bar includes links for Admin, Applications, Connectivity, Dashboard, Reports, Settings, and UCP. The page title is 'Add CUSTOM Extension'. Below the title are tabs for General, Voicemail, Find Me/Follow Me, Advanced, Zulu, and Other. The 'General' tab is selected. The form contains several sections: 'Add Extension' with fields for 'User Extension' (101), 'Display Name', and 'Outbound CID'; 'Language' with a 'Language Code' dropdown set to 'Default'; and 'User Manager Settings' with fields for 'Link to a Default User' (Create New User), 'Username' (John\_Doe), 'Password For New User' (da05532aa7dc95ab585c2df289a7b977), and 'Groups' (All Users).

При настройке внутренних номеров также следует ограничивать IP-адреса, которые могут быть на них зарегистрированы вплоть до пула адресов локальной подсети. IP-ATC Asterisk имеет встроенные **ACL (Access Control List)**, в настройке **sip.conf**. При помощи команд **permit/deny** можно разрешить лишь определенное количество IP-адресов для регистрации.

3. Другой важной мерой по усилению безопасности, является ограничение удаленного доступа к IP-ATC при помощи **firewall**. Будьте внимательны, так как в данном случае, главное грамотно настроить правила, по которым будет отрабатывать **firewall**. Убедитесь, что настройка не блокирует порты, которые использует ваша IP-ATC и не позволяет анонимно посылать ICMP запросы из публичной сети. Если вы планируете предоставлять удаленный доступ для авторизованных сотрудников, лучше всего организовать его при помощи VPN сервера (например, **OpenVPN**).
4. Если это возможно, то желательно использовать **NAT (Network Address Translation)**. При помощи NAT'a, можно присвоить IP-ATC приватный IP-адрес и существенно усложнить доступ к ней из Интернета.
5. Еще одним очень важным фактором, является разделение входящих и исходящих маршрутов (**Inbound Routes** и **Outbound Routes**). Необходимо, чтобы каждый маршрут принадлежал собственному контексту обработки вызова.
6. Отключите каналы и сервисы, которые не используются. Например, если вы не используете протокол **MGCP** или **skinny**. Отключить эти модули можно в **/etc/modules.conf** как показано ниже:

```
noload => chan_mgcp.so
noload => chan_skinny.so
noload => chan_oss.so
```

7. Чтобы усложнить работу всевозможным SIP-сканерам, необходимо в настройках **sip.conf** выставить следующее условие - **alwaysauthreject=yes**. Это будет препятствовать получению информации об использующихся внутренних номерах на вашей IP-ATC.
8. Рекомендуем создавать отдельные маршруты на звонки за рубеж (по сути, международное направление 810). Ставьте ограничения на звонки в таких маршрутах или закрывайте их PIN – кодом, который могут знать только сотрудники вашей организации.

## Какие порты открыть для Asterisk/FreePBX

Расскажем про сетевые порты, которые необходимо открыть на вашем фаерволе для корректного пользовательского доступа и работы оконечных устройств. В разделе указаны дефолтные и порты, и, с точки зрения безопасности, мы рекомендуем их сменить на нестандартные.

### Доступ администратора системы

| Порт  | Транспорт (UDP/TCP) | Назначение                               | Смена порта   | Безопасность  | Дополнительно  |
|---|---------------------|--|---|---|--|
| 22  | TCP                 | Подключение к SSH консоли                | Может быть изменен только через Linux CLI   | Не рекомендуется оставлять порт открытым в публичную сеть (не вызывающую доверие) | Порт используется для SSH подключения к АТС извне  |
| 80<br><b>FreePBX</b><br><b>X</b><br>2001<br><b>PBXact</b> | TCP                 | Графический интерфейс по HTTP (не HTTPS) | Можно поменять через графический интерфейс по пути <b>System Admin &gt; Port Management</b> | Не рекомендуется оставлять порт открытым в публичную сеть (не вызывающую доверие) | Используется для пользовательского доступа к WEB - интерфейсу АТС                            |
| 443   | TCP                 | Графический интерфейс по HTTPS           | Можно поменять через графический интерфейс по пути <b>System Admin &gt; Port Management</b> | Не рекомендуется оставлять порт открытым в публичную сеть (не вызывающую доверие) | Используется для пользовательского доступа к WEB - интерфейсу АТС. Использует SSL шифрование |

Admin
Applications
Connectivity
Dashboard
Reports
Settings
UCP
Основные
Trunk Balance

### System Admin

#### Port Management

This allows you to set port numbers for various services. The available ports you can configure are as follows:

- Admin - Administration for this system (This interface). Default port 80. (Can not be disabled)
- UCP - User Control Panel. Default port 81
- HTTP Provisioning - Access to provisioning files. Default port 84
- RESTful API - Default port 83
- RESTful Phone Apps - Default port 82

| Service Name       | Insecure Port (http) | Secure Port (https) |
|--------------------|----------------------|---------------------|
| Admin              | Port 80 (Default)    | Port 443 (Default)  |
| UCP                | Port 81 (Default)    | Disabled            |
| HTTP Provisioning  | Port 83              | Port 1443 (Default) |
| RESTful API        | Port 85              | Disabled            |
| RESTful Phone Apps | Port 84              | Port 3443 (Default) |

DNS
Intrusion Detection
Network Settings
Hostname
Notifications Settings
Power Options
**Port Management**
PnP Configuration
HTTPS Setup
Time Zone

## Доступ для SIP/IAX устройств

| Порт | Транспорт (UDP/TCP) | Назначение  | Смена порта  | Безопасность  | Дополнительно                                       |
|------|---------------------|---|--|---|---|
| 5060 | UDP                 | Порт получения телефонной сигнализации модулем <b>chan_PJSIP</b>            | Есть возможность изменить порт в рамках графического интерфейса АТС в модуле <b>SIP Settings</b> | Не рекомендуется оставлять порт открытым в публичную сеть (не вызывающую доверие) | Стандартный порт для сигнализации модуля chan_PJSIP |
| 5061 |                     | Порт получения защищенной телефонной сигнализации модулем <b>chan_PJSIP</b> | Есть возможность изменить порт в рамках графического интерфейса АТС в модуле <b>SIP Settings</b> | Не рекомендуется оставлять порт открытым в публичную сеть (не вызывающую доверие) | Защищенный порт для сигнализации модуля chan_PJSIP  |
| 5160 | UDP                 | Порт получения телефонной сигнализации модулем <b>chan_SIP</b>              | Есть возможность изменить порт в рамках графического интерфейса АТС в модуле <b>SIP Settings</b> | Не рекомендуется оставлять порт открытым в публичную сеть (не вызывающую доверие) | Стандартный порт для сигнализации модуля chan_SIP   |

|             |     |   |  |  |   |
|-------------|-----|---|--|--|---|
| 5161        |     | Порт получения защищенной телефонной сигнализации модулем <b>chan_SIP</b> | Есть возможность изменить порт в рамках графического интерфейса АТС в модуле <b>SIP Settings</b> | Не рекомендуется оставлять порт открытым в публичную сеть (не вызывающую доверие)  | Защищенный порт для сигнализации модуля chan_SIP                        |
| 10000-20000 | UDP | Получение <b>RTP</b> потока в рамках SIP сессии                           | Есть возможность изменить порт в рамках графического интерфейса АТС в модуле <b>SIP Settings</b> | Можно открывать данные диапазон и, зачастую, это является требование SIP - провайдеров (RTP трафик зачастую приходит с различных IP - адресов) | Порты, необходимые для голосовой составляющей телефонного звонка        |
| 4569        | UDP | Работа протокола <b>IAX</b>   | Есть возможность изменить порт в рамках графического интерфейса АТС в модуле <b>SIP Settings</b> | Не рекомендуется оставлять порт открытым в публичную сеть (не вызывающую доверие)  | Используется для транкового объединения серверов и оконечных устройств. |

## Доступ к UCP (User Control Panel)

| Порт | Транспорт (UDP/TCP) | Назначение                                   | Смена порта   | Безопасность   | Дополнительно   |
|------|---------------------|--|---|--|---|
| 81   | TCP                 | Графический интерфейс UCP по HTTP (не HTTPS) | Порт можно поменять через <b>FreePBX в System Admin &gt; Port Management</b>                                      | Не рекомендуется оставлять порт открытым в публичную сеть (не вызывающую доверие). Для удаленных пользователей используйте HTTPS | Порт доступа к пользовательской панели <b>UCP</b>   |
| 4443 | TCP                 | Графический интерфейс UCP по HTTPS           | Порт можно поменять через <b>FreePBX в System Admin &gt; Port Management</b>                                      | Можно оставлять открытым в сеть, так как трафик зашифрован, а так же происходит аутентификация пользователей                     | Порт доступа к пользовательской панели UCP с помощью <b>SSL</b> шифрования                    |
| 8088 | TCP                 | Порт для WebRTC клиентов                     | Порт можно поменять через FreePBX в <b>Advanced Settings &gt; Asterisk Builtin mini-HTTP &gt; HTTP Bind Port</b>  | Не рекомендуется оставлять порт открытым в публичную сеть (не вызывающую доверие). Для удаленных пользователей используйте HTTPS | Необходим для реализации WebRTC звонков через UCP (звонок через браузер)                      |
| 8089 | TCP                 | Порт для шифрования WebRTC клиентов          | Порт можно поменять через FreePBX в <b>Advanced Settings &gt; Asterisk Builtin mini-HTTP &gt; HTTPS Bind Port</b> | Можно оставлять открытым в сеть, так как трафик зашифрован, а так же происходит аутентификация пользователей                     | Необходим для реализации <b>WebRTC</b> звонков с шифрованием через UCP (звонок через браузер) |
| 8001 | TCP                 | Node Server - получение                      | Порт можно поменять   | Не рекомендуется оставлять порт  | Процесс отвечает за real - time   |



|      |     |  |   |  |   |
|------|-----|--|---|--|---|
|      |     | информации в реальном времени в рамках UCP | через FreePBX в <b>Advanced Settings &gt; UCP NodeJS Server &gt; NodeJS Bind Port</b>                           | открытым в публичную сеть (не вызывающую доверие)  | активности: всплывающая информация, чаты и прочее                                 |
| 8003 | TCP | Node Server (защищенные подключения)       | Порт можно поменять через FreePBX в <b>Advanced Settings &gt; UCP NodeJS Server &gt; NodeJS HTTPS Bind Port</b> | Можно оставлять открытым в сеть, так как трафик зашифрован, а так же происходит аутентификация пользователей | Процесс отвечает за real - time активности: всплывающая информация, чаты и прочее |

Остальные порты зависят от ваших конкретных требований: наличие **RMS** компонента мониторинга, **Zulu**, функционала провизионинга (**EPN**) и прочие.

## FreePBX - обнаружение слабых паролей

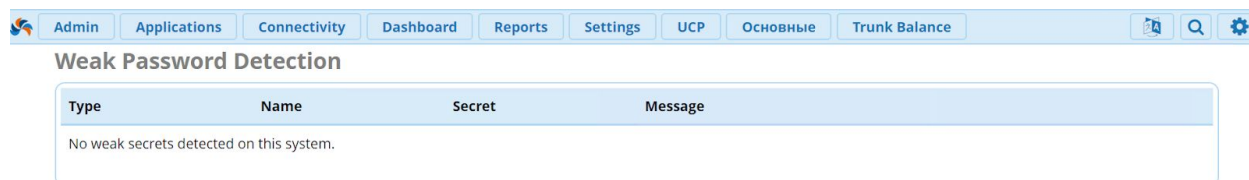
Как известно, сильный пароль – это очень важная составляющая безопасности любого актива, к которому, тем или иным образом можно получить доступ. Не даром все best practices начинаются с рекомендаций устанавливать сильный, устойчивый к взлому пароль. В данном разделе мы будем говорить о прописных истинах, поэтому её можно считать скорее «дружеским советом» для тех, кто только начинает своё знакомство с FreePBX.

Слабый пароль, неважно где – это большой риск, который нельзя оставлять без внимания и следует немедленно устранить.

### Обзор

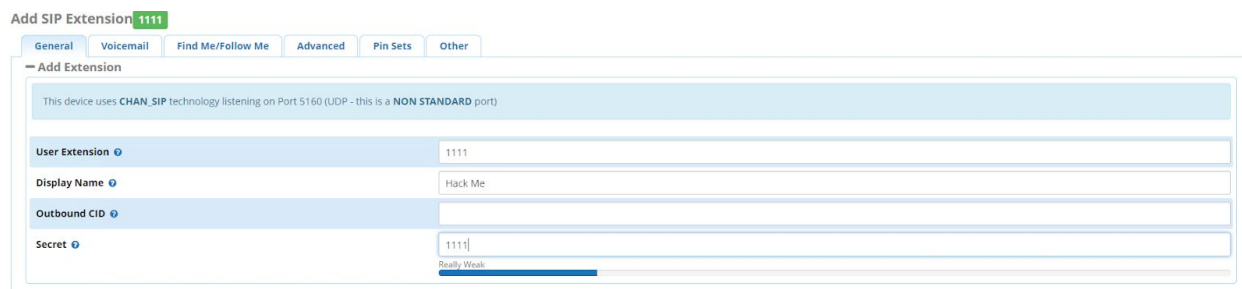
Начиная с версии 13 во FreePBX появился модуль **Weak Password Detection** который автоматически детектирует и сообщает о том, что в системе имеется слабый пароль, а также указывает, где именно он обнаружен: на внутреннем номере (**Extension**), транке (**Trunks**), конференц - комнате (**Conferences**) и других модулях.

Чтобы проверить, имеется ли у вас в системе слабый пароль, откройте вкладку Reports → Weak Password Detection. Вот как должно выглядеть окно данного модуля у всех без исключения (окно нормального человека):

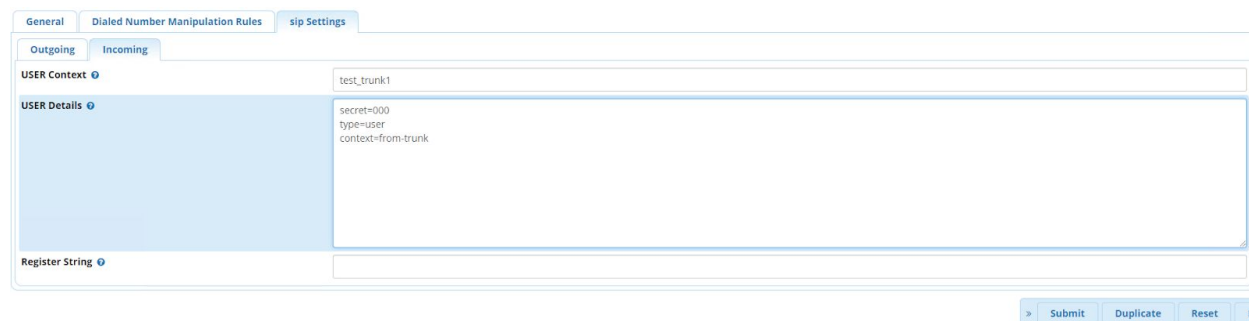


Данное сообщение говорит нам о том, что у нас в системе нет слабых паролей. А теперь, давайте-ка немножко похулиганим и создадим пару сущностей с очень слабыми паролями и посмотрим что из этого выйдет.

Наплевав на все **best practices**, создадим внутренний номер 1111 с паролем **1111**:



А ещё создадим транк с паролем **000**:



А теперь отправляемся в модуль **Weak Password Detection** и перед нами открывается «окно курильщика». Вот так не должно быть никогда:

Admin

Applications

Connectivity

Dashboard

Reports

Settings

UCP

## Weak Password Detection

| Type      | Name        | Secret | Message                        |
|-----------|-------------|--------|--------------------------------|
| Extension | 1111        | 1111   | Secret has consecutive digit 1 |
| SIP Trunk | test_trunk  | 000    | Secret less than 6 digits      |
| SIP Trunk | test_trunk1 | 000    | Secret less than 6 digits      |

Помимо этого, нам будут напоминать о слабых паролях в **Dashboard'e**:

System Overview

Добро пожаловать в FreePBX

FreePBX 14.0.1.24 'VoIP Server'

(Вы можете изменить это имя в Дополнительных Настройках)

Краткая сводка

Астериск ✓

Firewall Configuration ✓

Сервер MySQL ✓

Fail2Ban ✓

System Registration ✓

Веб сервер ✓

System Firewall ✓

Restapps Daemon ✓

UCP Daemon ✓

Xmpp Daemon ✓

Сист. информация обновлена 10 секунд назад

⚠ Проблема безопасности ⚠

3 на внутреннем номере/транке установлен слабый пароль

Этот важный вопрос нужно решить срочно

3 на внутреннем номере/транке установлен слабый пароль

2 Новый модуль доступен

Default bind port for CHAN\_PJSIP is: 5060, CHAN\_SIP is: 5160

Показать все

Как только Вы настроите внутреннюю нумерацию, линии к провайдерам (транки), пользовательский доступ, не поленитесь, зайдите лишний раз в модуль **Weak Password Detection** и если там будет уведомление о слабом пароле в системе – незамедлительно смените его! Но помните, что сильный пароль – это не гарантия безопасности, это всего

лишь один из уровней, который должен применяться в комплексе с остальными мероприятиями по защите системы.

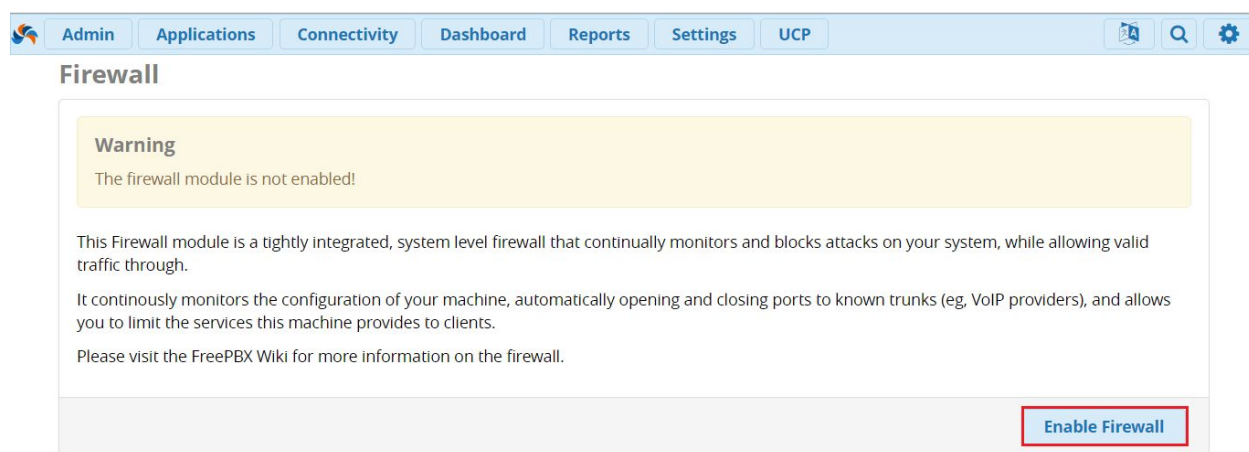
## Конфигурация Firewall в FreePBX

Рассмотрим модуль, который стал доступен во FreePBX только с версии 13 и который позволяет создать первичную низкоуровневую защиту нашей IP-АТС - Firewall. Нужно отметить, что попытки создать нечто подобное на ранних версиях FreePBX всё-таки были, но все они не увенчались успехом и заставляли пользователей так или иначе идти на компромиссы для сохранения доступности функционала IP-АТС. Модуль **Firewall** был разработан с глубоким пониманием существующих проблем и его основной целью является защита “**средней**”, или другими словами, типовой инсталляции при обязательном сохранении VoIP сервисов.

Данный модуль отслеживает и блокирует атаки, пропуская при этом разрешенный трафик, а также непрерывно контролирует конфигурацию системы, автоматически открывая и закрывая порты для необходимых транков.

### Настройка модуля Firewall

Перейдем к настройке. Для того, чтобы попасть в модуль, нужно перейти по следующему пути: **Connectivity** -> **Firewall**, откроется следующее окно:

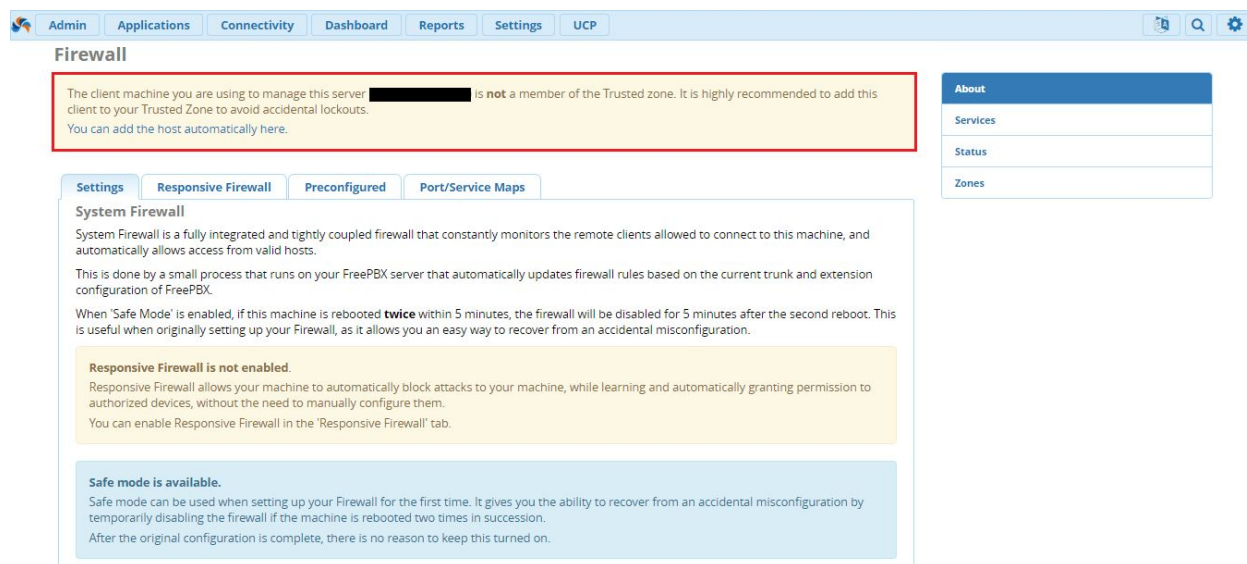


FreePBX is a registered trademark of Sangoma Technologies Inc.  
FreePBX 13.0.167 is licensed under the GPL  
Copyright© 2007-2016

<http://merionet.ru/>

Чтобы включить модуль, нажмите кнопку Enable Firewall. Обратите внимание, после включения модуля никакие правила еще не задействованы, их нужно настроить.

Первое о чём сообщает модуль, это то, что IP-адрес, под которым мы зашли на IP-АТС не является членом “зоны доверия” (**Trusted Zone**) и предлагает добавить его для исключения возможных блокировок:



Для наибольшего понимания, давайте разберёмся с понятием зоны (Zone), которым оперирует модуль Firewall.

Все сетевые соединения, поступающие на **VoIP-сервер** считаются частью зоны. Каждый сетевой интерфейс и данные, поступающие на него принадлежат к определенной зоне. Стандартные зоны делятся на следующие:

- **Reject** - Все соединения, относящиеся к данной зоне, запрещены. Обратите внимание, что эта зона по-прежнему принимает RTP трафик, но никакие другие порты по умолчанию не прослушиваются. Трафик данной зоны может быть обработан с помощью Responsive Firewall, о котором будет сказано далее.
- **External** - Позволяет только https соединения для доступа к интерфейсу управления и UCP порту, если они определены. Трафик данной зоны может также быть обработан с помощью Responsive Firewall
- **Other** - Используется на доверенных внешних сетях, или других хорошо известных сетях. По умолчанию, позволяет получить доступ к UCP, а также обеспечивает нефильтрованный SIP и IAX.

- **Internal** - Используется на внутренних локальных сетях, по умолчанию позволяет получить доступ ко всем сервисам IP-АТС.
- **Trusted** - Все сетевые соединения данной зоны разрешены. Пропускается весь трафик от доверенной зоны. Именно сюда нам предложат добавить наш IP-адрес при первом включении модуля.

Итак, чтобы добавить наш IP-адрес в список доверенных, нужно нажать **You can add the host automatically here.**

**Firewall**

The client machine you are using to manage this server [redacted] is not a member of the Trusted zone. It is highly recommended to add this client to your Trusted Zone to avoid accidental lockouts.  
 You can add the host automatically here.

**Settings** Responsive Firewall Preconfigured Port/Service Maps

**System Firewall**  
 System Firewall is a fully integrated and tightly coupled firewall that constantly monitors the remote clients allowed to connect to this machine, and automatically allows access from valid hosts.  
 This is done by a small process that runs on your FreePBX server that automatically updates firewall rules based on the current trunk and extension configuration of FreePBX.  
 When 'Safe Mode' is enabled, if this machine is rebooted **twice** within 5 minutes, the firewall will be disabled for 5 minutes after the second reboot. This is useful when originally setting up your Firewall, as it allows you an easy way to recover from an accidental misconfiguration.

**Responsive Firewall is not enabled.**  
 Responsive Firewall allows your machine to automatically block attacks to your machine, while learning and automatically granting permission to authorized devices, without the need to manually configure them.  
 You can enable Responsive Firewall in the 'Responsive Firewall' tab.

**Safe mode is available.**  
 Safe mode can be used when setting up your Firewall for the first time. It gives you the ability to recover from an accidental misconfiguration by temporarily disabling the firewall if the machine is rebooted two times in succession.  
 After the original configuration is complete, there is no reason to keep this turned on.

**About**  
 Services  
 Status  
 Zones

Мы попадаем во вкладку **Preconfigured**. Предлагается два варианта, это добавление адреса хоста и добавление подсети **Add Host** и **Add Network** соответственно:

**Firewall**

The client machine you are using to manage this server [redacted] is not a member of the Trusted zone. It is highly recommended to add this client to your Trusted Zone to avoid accidental lockouts.  
 You can add the host automatically here.

**Settings** Responsive Firewall **Preconfigured** Port/Service Maps

This allows you to simply add a pre-configured set of networks to your trusted zone. Once you have added your selections, you can fine-tune them, if required, on the Networks tab.

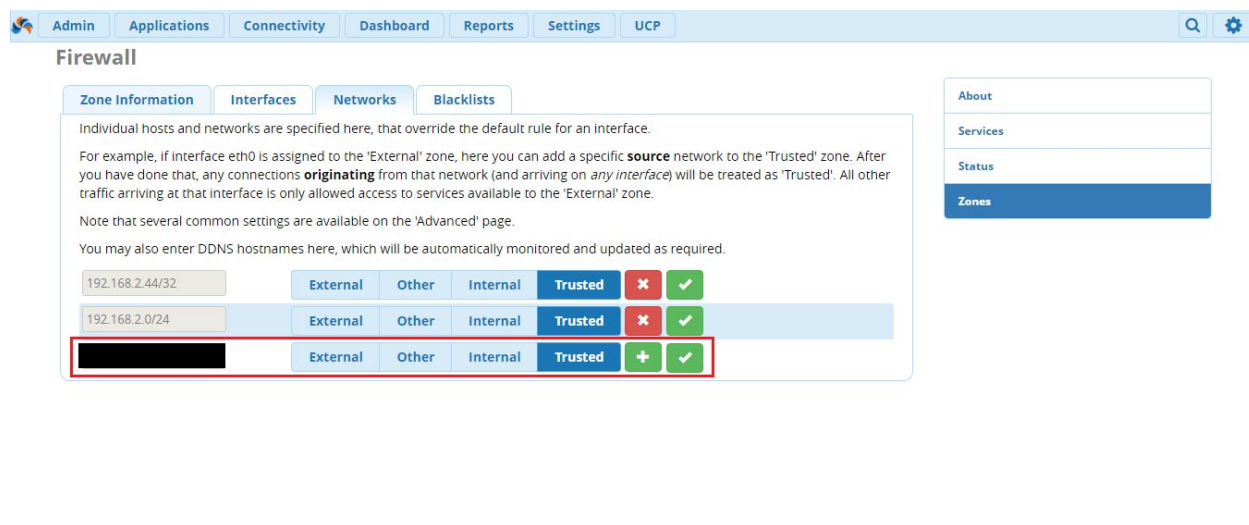
**RFC1918/RFC4193**  
 RFC1918 and RFC4193 are the RFCs that define the reserved, internal, network address space to be used when you're not directly connected to the internet, or do not want your address space routable. This adds the IPv4 networks 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8 and IPv6 networks fc00::/8 and fd00::/8 to the 'Trusted' zone, and excludes it from all firewalls.  
**Important Warning!** If you are in a hosted environment (for example, AWS) and you enable this, you may be inadvertently allowing other hosted clients unrestricted access to your machine! Please use common sense to make sure that you are only allowing known trusted networks.  
 Add to Trusted

**Your Client**  
 This explicitly grants permission to the machine that is managing the firewall service now. If you select 'Add Network', it will add the entire network that the server sees you coming from [redacted] or if you select 'Add Host' it will only add the individual IP address (91.77.52.122/32). When starting to configure your firewall, it is wise to enable this to ensure you don't lock yourself out of your machine.  
 If you are coming from an IPv6 Network, it **not recommended** to only add your 'Host', as MAC address changes, or IPv6 Security Extensions, will randomly and unexpectedly change your IP address. Ensure you add the complete network.  
 Add Host Add Network

**About**  
 Services  
 Status  
 Zones

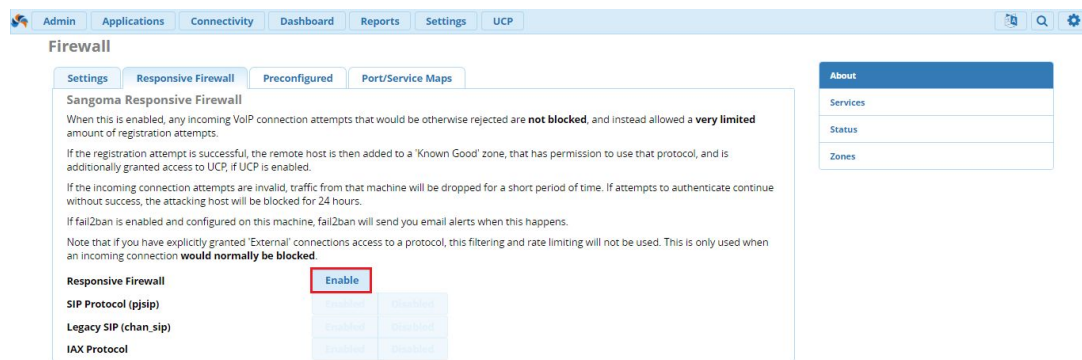


Проверить, что адрес (или сеть) добавлены в список доверенных можно во вкладке **Zones** в разделе **Networks**.

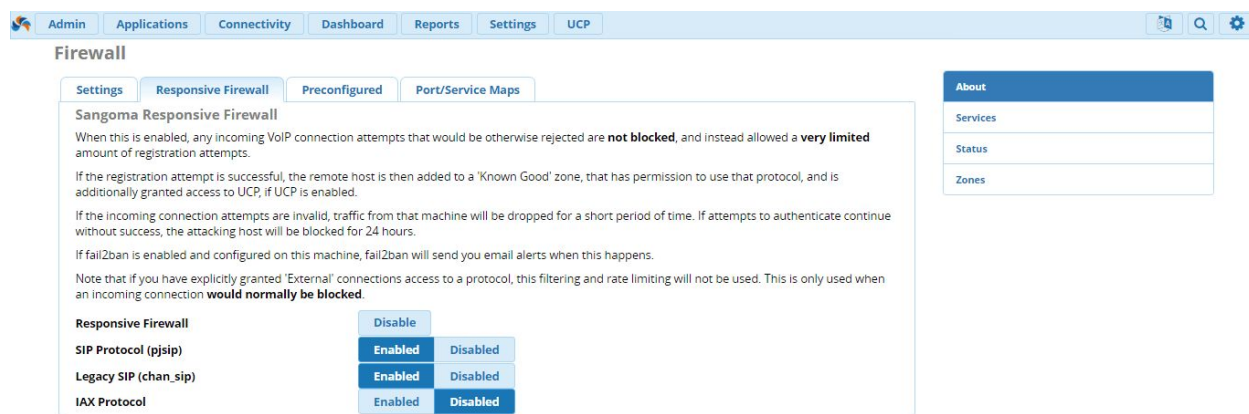


В модуле **Firewall** есть также дополнительный элемент, который отслеживает сигнализационные запросы определенных сервисов и блокирует возможные атаки - **Responsive Firewall**. Такими запросами могут быть запросы протоколов сигнализации SIP или IAX, например, запросы авторизации или вызова. Когда Responsive включен, то любой сигнализационный пакет исходящий от хоста проходит через Firewall, если после некоторого количества таких пакетов, хост отправлявший их не прошёл успешную регистрацию, то весь трафик от этого хоста сбрасывается на короткий промежуток времени (60 сек). Если после данной блокировки хост продолжает слать пакеты с запросом регистрации и безуспешно пытается зарегистрироваться, то блокируется уже его IP-адрес на 24 часа. Кроме того, если на сервере настроен fail2ban, то система ещё и письмо отправит о данном событии.

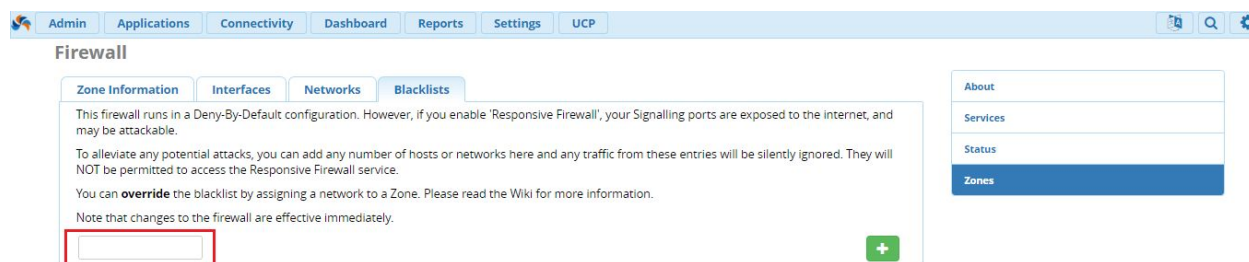
Чтобы включить данный функционал, на вкладке **Responsive** нужно нажать на кнопку **Enable**:



Далее необходимо указать, для каких протоколов должен работать данный функционал:



Известные IP-адреса или даже целые подсети, которые проявляли подозрительную активность и которые не должны иметь доступа к IP-ATC можно заблокировать во вкладке **Zones -> Blacklists**.



И последний по счёту, но не по значимости, функционал модуля Firewall, о котором хотелось бы рассказать - **Safe Mode**. Данный функционал позволяет получить доступ к IP-ATC если случайно была применена неправильная конфигурация, которая привела к потере доступа, а доступа к консоли у вас нет.



Admin
Applications
Connectivity
Dashboard
Reports
Settings
UCP

## Firewall

Settings
Responsive Firewall
Preconfigured
Port/Service Maps

### System Firewall

System Firewall is a fully integrated and tightly coupled firewall that constantly monitors the remote clients allowed to connect to this machine, and automatically allows access from valid hosts.

This is done by a small process that runs on your FreePBX server that automatically updates firewall rules based on the current trunk and extension configuration of FreePBX.

When 'Safe Mode' is enabled, if this machine is rebooted **twice** within 5 minutes, the firewall will be disabled for 5 minutes after the second reboot. This is useful when originally setting up your Firewall, as it allows you an easy way to recover from an accidental misconfiguration.

**Responsive Firewall is enabled.**

There is no need to explicitly add definitions for peers, as they are automatically allowed through the firewall after successfully registering. After an endpoint is registered, the source of that endpoint is **automatically granted** permission to use UCP, if UCP is enabled.

**Safe mode is available.**

Safe mode can be used when setting up your Firewall for the first time. It gives you the ability to recover from an accidental misconfiguration by temporarily disabling the firewall if the machine is rebooted two times in succession. After the original configuration is complete, there is no reason to keep this turned on.

System Firewall

Disable Firewall

Safe Mode

Available

Disabled

Firewall Wizard

Re-Run Wizard

Filter Type

Reject

Drop

### About

Services

Status

Zones

При включении модуля Firewall, Safe Mode уже доступен, но чтобы его активировать, необходимо **дважды** перезапустить систему. Сначала необходимо выполнить перезапуск один раз, дождаться, пока сервер полностью загрузится, а затем произвести вторую перезагрузку. После чего, система отложит загрузку правил Firewall'a, а вы сможете спокойно убраться ту конфигурацию, из-за которой потеряли доступ.

О том, что система находится в **Safe Mode**, будет говорить огромное уведомление в самом верху страницы, которое исчезнет через пять минут, тогда же запустятся правила Firewall.

## Firewall

### Firewall has not started yet!

As this machine has recently been rebooted, the firewall is **temporarily** running in Safe Mode, with no rules applied.

This allows you to perform emergency repairs to the firewall, in case you're accidentally locked out. The firewall will start automatically after this machine has been running for more than 5 minutes.

Any changes you make will be saved, but will not take effect until the firewall is started.

### About

Services

Status

Zones

Settings
Responsive Firewall
Preconfigured
Port/Service Maps

### System Firewall

System Firewall is a fully integrated and tightly coupled firewall that constantly monitors the remote clients allowed to connect to this machine, and automatically allows access from valid hosts.

This is done by a small process that runs on your FreePBX server that automatically updates firewall rules based on the current trunk and extension configuration of FreePBX.

When 'Safe Mode' is enabled, if this machine is rebooted **twice** within 5 minutes, the firewall

## Настройка SSL в FreePBX

Для управления сертификатами SSL в графическом интерфейсе FreePBX создан специальный модуль - **Certificate Management**. Но, перед тем как перейти к его настройке, давайте вспомним, для чего же нужен сертификат и что же такое SSL в Asterisk?

### SSL и FreePBX

Сертификат SSL позволяет вашему FreePBX иметь уникальную цифровую подпись, с помощью которой, каждый раз при обращении к интерфейсу будет создаваться защищенное соединение между web – сервером и клиентским устройством. SSL сертификат включает в себя информацию о его владельце и открытый ключ. Выдачей SSL сертификатов занимается специальный центр сертификации (Certification authority), честность которого априори неоспорима.

Помимо этого, сертификат позволяет совершать звонки по защищенному транспортному протоколу TLS и шифровать голосовые потоки через SRTP.

### Генерация CSR

Приступаем к получению сертификата. Центр сертификации попросит вас предоставить сгенерированный CSR файл (Certificate Signing Request). Это является обязательной частью подачи заявления на сертификат, и содержит в себе различные данные об организации, такие как наименование, полное имя домена, код страны и прочие.

Перейдем во вкладку **Admin -> Certificate Management**. В открывшемся окне модуля нажимаем + Generate CSR. Откроется окно генерации CSR файла:

| New Certificate Signing Request |                |
|---------------------------------|----------------|
| Name                            | MerionNetworks |
| Common Name (Host Name) (CN)    | merionet.ru    |
| Organization Name (O)           | MerionNetworks |
| Organization Unit (OU)          | IT             |
| Country (C)                     | RU             |
| State/Province (ST)             | Wisconsin      |
| City or Locality (L)            | Moscow         |

Разберемся поподробнее с каждым из пунктов:

- **Name** - имя для сгенерированного CSR файла. Когда файл будет сгенерирован, он будет иметь название, как указано в этом поле
- **Common Name (Host Name) (CN)** - полное имя домена
- **Organization Name (O)** - полное наименование организации, как указано в учредительных документах
- **Organization Unit (OU)** - наименование подразделения (отдела), на который выписывается данный сертификат
- **Country (C)** - код страны из двух букв. В нашем случае RU.
- **State/Province (ST)** - наименование области или края, в котором вы находитесь. В нашем случае мы оставили это поле пустым
- **City or Locality (L)** - укажите город. Мы указали Moscow

По окончании настроек нажмите **Generate CSR**. После того, как CSR файл будет сгенерирован, он станет доступен для скачивания в главном интерфейсе модуля. Для его загрузки, нажмите на кнопку **Download CSR**. Сам файл представляет из себя ключ, заключенный в теги начала и окончания:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0zCCABsCAQAwY0xFDASBgNVBAMTC211cm1vbWV0LnJ1MRgwFgYDVQKKEw9N
ZXJpb24gTmV0d29ya3MxCzAJBgNVBAsTAK1UMQswCQYDVQQGEwJSVTEMMaoGA1UE
CBMDUUXEMQ8wDQYDVQQHEwZNb3Njb3cxIjAgBgkqhkiG9w0BCQEWEludmFsaWRA
ZXhhbXBsZS5jb20wgGEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDKvJYr==
-----END CERTIFICATE REQUEST-----
```

После этого, вам необходимо написать заявление в центр сертификации и приложить к нему этот файл, после чего вы сможете получить свой SSL сертификат.

## Загрузка сертификата

После того, как мы получили сертификат от сертификационного центра (CA), его необходимо загрузить на сервер. Нажимаем на кнопку New Certificate и выбираем Upload Certificate

The screenshot shows a web interface for adding a new certificate. The form is titled 'Add New Certificate' and has a navigation bar at the top with links to Admin, Applications, Connectivity, Dashboard, Reports, Settings, and UCP. The form fields are as follows:

- Name:** MerionNetworks
- Description:** For test
- Passphrase:** (masked with dots)
- CSR Reference:** MerionNetworks
- Certificate:** A large text area containing a sample certificate text: 

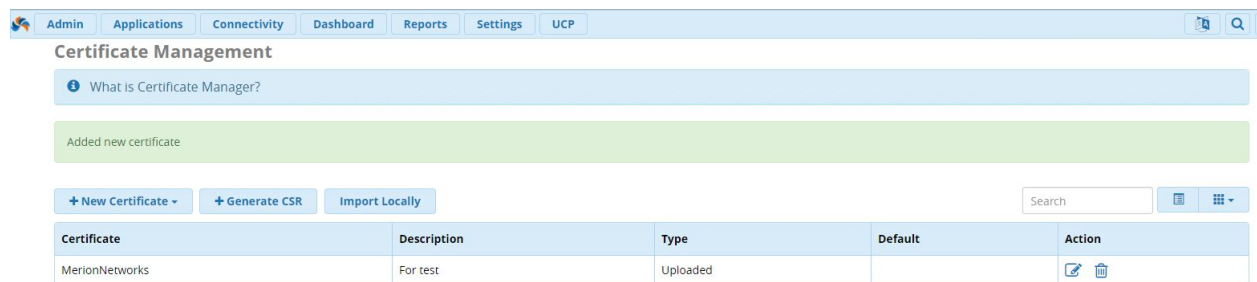
```
-----BEGIN CERTIFICATE-----
Soemlaxoac0lemOuwr1ewriaturlucisLudroApOluBriAcSenLeGoef7apRoarl
chou2i5zLux4uchia0LAzoAspleHou9l3led8espijlablevi2C5iumoAbIUwrl
woU5piuvoakiadi1gOaSTLuqlurieyouh0ezlax58goeip85SoaswumliUw0lewi
9plewIA5lehu3l9sw692iusPIAchoezSWiufieciaqlunlemiAno0StoEFrluR
-----END CERTIFICATE-----
```
- Trusted Chain:** A large text area with the placeholder 'Paste new certificate here'.

At the bottom right of the form are two buttons: 'Generate Certificate' and 'Reset'.

- **Name** - имя для сертификата
- **Description** - описание сертификата. Используется только внутри модуля и не влияет на импорт сертификата.
- **Passphrase** - кодовая фраза, то есть пароль. Необходима для доступа к сертификату и генерации сертификатов на стороне клиента. Если вы не укажете пароль в данном поле, то вам придется указывать его каждый раз, когда потребуется новый сертификат. К тому же, отсутствие пароля приводит к незащищенности приватного ключа сертификата.
- **CSR Reference** - в данном поле выберите сгенерированный CSR файл на предыдущем этапе.
- **Поле Certificate** - откройте файл сертификата, который вам предоставил сертификационный центр и полностью копируйте его в это поле, начиная от тэга «-----BEGIN CERTIFICATE-----» до «-----END CERTIFICATE-----»
- **Поле Trusted Chain** - порой, центр сертификации (CA), помимо самого сертификата может предоставить вам целый набор файлов. Они называется Trusted Chain, то

есть цепочки доверия. Последовательно откройте каждый из файлов и скопируйте их содержимое в это поле.

По окончании настроек нажмите **Generate Certificate**. По окончании настроек вы сможете увидеть ваш сертификат в общем списке. В процессе эксплуатации он доступен для редактирования:



## Бесплатный сертификат Let's Encrypt

Интерфейс FreePBX имеет встроенную возможность настройки бесплатного SSL сертификата с помощью сертификационного центра Let's Encrypt. Чтобы воспользоваться бесплатным сертификатом, у вашего сервера должно быть настроено доменное имя, и его оно должно резолвиться по его IP – адресу

Помимо этого, следующие хосты должны быть добавлены в разрешенные в настройках фаервола:

1. outbound1.letsencrypt.org
2. outbound2.letsencrypt.org
3. mirror1.freepbx.org
4. mirror2.freepbx.org

## Лучшие практики по защите SSH подключения

**OpenSSH** позволяет выполнять удаленное подключение к серверу, производить манипуляции с файлами и управлять системой. Сегодня хотим рассказать про лучшие методы, которые позволяют увеличить безопасность системы на базе OpenSSH.

### Конфигурационные файлы

- **/etc/ssh/sshd\_config** - файл конфигурации сервера OpenSSH;
- **/etc/ssh/ssh\_config** - файл конфигурации клиентской части OpenSSH;
- **~/.ssh/** - директория, в которой хранятся пользовательские SSH настройки;
- **~/.ssh/authorized\_keys** или **~/.ssh/authorized\_keys** - список ключей (RSA или DSA), которые используются для подключения к пользовательским аккаунтам;
- **/etc/nologin** - если данный файл существует в системе, то sshd запретит подключаться всем пользователям кроме root в систему;
- **/etc/hosts.allow** и **/etc/hosts.deny** - система запрета (часть безопасности). Работает по аналогии с ACL;
- **SSH порт по умолчанию** - 22

| Left                 | File     | Command | Options | Right  |
|----------------------|----------|---------|---------|--------|
| <                    | /etc/ssh |         |         | . [^]> |
| 'n                   | Name     | Size    | Modify  | time   |
| /..                  | UP--DIR  | Nov 29  | 10:55   |        |
| .sshd_config.swn     | 16384    | Dec 5   | 16:13   |        |
| .sshd_config.swo     | 16384    | Dec 5   | 16:05   |        |
| .sshd_config.swp     | 4096     | Dec 5   | 15:59   |        |
| moduli               | 125811   | Nov 13  | 2014    |        |
| ssh_config           | 2047     | Nov 13  | 2014    |        |
| ssh_host_dsa_key     | 668      | Sep 5   | 2016    |        |
| ssh_host_dsa_key.pub | 590      | Sep 5   | 2016    |        |
| ssh_host_key         | 963      | Sep 5   | 2016    |        |
| ssh_host_key.pub     | 627      | Sep 5   | 2016    |        |
| ssh_host_rsa_key     | 1675     | Sep 5   | 2016    |        |
| ssh_host_rsa_key.pub | 382      | Sep 5   | 2016    |        |
| sshd_config          | 3877     | Sep 5   | 2016    |        |

### Не нужен - выключай

Если вашему серверу не требуется удаленное подключение по SSH, то обязательно отключите его. В таких системах как **CentOS/RHEL** делается это так:

```
chkconfig sshd off
yum erase openssh-server
```

## Используйте SSH второй версии

Протокол SSH первой версии имеет проблемы с безопасностью, которые закрыты во второй версии. Поэтому, используйте вторую версию. Убедитесь, что в файле `/etc/ssh/sshd_config` указана опция **Protocol 2**.

## Ограничивайте SSH доступ

По умолчанию, все системные пользователи имеют возможность подключаться к системе по SSH. Рекомендуем ограничить SSH доступ в целях безопасности. Например, разрешить SSH для пользователей `root`, `merion` и `networks`:

```
AllowUsers root merion networks
```

С другой стороны, вы можете разрешить доступ всем пользователям, кроме указанных:

```
DenyUsers root merion networks
```

## Время неактивности

Важно указывать время, в течение которого, не активная сессия будет терминирована (завершена). Это можно сделать следующими опциями:

```
ClientAliveInterval 300
ClientAliveCountMax 0
```

В данной настройке мы указали время бездействия равным 300 секунд (5 минут).

## Про файлы `.rhosts`

Дело в том, что данный файл содержит список хостов и пользователей. Если в данном файле содержится комбинация хоста и юзера, то данный пользователь сможет подключиться к системе по SSH без запроса пароля. Рекомендуем отключить эту «замечательную» фичу:

```
IgnoreRhosts yes
```

## Никакой аутентификации на базе хоста!

Так называемая **Host-Based Authentication** позволяет пользователю с определенного хоста подключаться к серверу. Отключаем:

```
HostbasedAuthentication no
```

## Прямое подключение через root

Не нужно открывать root. Максимум, советуем использовать прямое root подключение на время проведения работ. Затем отключать. Лучше давать su (sudo) доступ для некоторых категория пользователей. Закрывать можно вот так:

```
PermitRootLogin no
```

## Сделайте баннер

Для каждого подключающегося [сделайте баннер](#), в котором можно угрожать злоумышленникам, которые пытаются совершить несанкционированный доступ. За настройку баннера отвечает параметр Banner.

## 22 порт только изнутри!

Сделайте доступ к 22 порту системы только через цепочку фаервол правил. Лучше всего, оставить доступ только изнутри LAN. Например, в Iptables можно дать доступ для 192.168.11.0/24:

```
-A RH-Firewall-1-INPUT -s 192.168.11.0/24 -m state --state NEW -p tcp --dport 22 -j ACCEPT
```

## Где слушать

По умолчанию SSH слушает подключения на всех доступных интерфейсах. Мы рекомендуем сменить порт по умолчанию и указать IP – адрес, на котором необходимо ожидать подключения. Например, мы укажем порт 962 и IP – адрес 192.168.11.24

```
Port 962  
ListenAddress 192.168.11.24
```



## Запретить пустые пароли

Бывают пользователи без паролей. Их доступ к SSH так же необходимо запретить с помощью опции:

```
Port 962
PermitEmptyPasswords no
```

## Анализируйте логи

Установите логирование событий в режим **INFO** или **DEBUG** – это позволит иметь расширенный контроль над системой:

```
LogLevel INFO
```

## Генератор устойчивых паролей

Для всех паролей, где подсистема генерации не подразумевает создание устойчивого к взлому пароля, мы разработали [генератор устойчивых паролей](#), который по одному клику сделает для вас устойчивый к взлому пароль.

Ваш криптостойкий пароль

Выберите все опции и получите пароль :)

Длина пароля?

10

Какие символы используем?

~ ! @ # \$ % ^ & \* ( ) - \_ + = { } [ ] ; : ?

Маленькие буквы?

Нет ☒ Да

Большие буквы?

Нет ☒ Да

Цифры в пароле?

Нет ☒ Да **НЕХ?**

Специальные символы?

Нет ☒ Да

Символы могут повторяться?

Нет ☒ Да

ГЕНЕРИРОВАТЬ

ОБНУЛИТЬ

[Генератор доступен по ссылке](#). Добавьте его в закладки браузера - при генерации паролей для транков, внутренних номеров, SSH/FTP/WEB или иного доступа, воспользуйтесь им.

## Домашнее задание N°4

В окончание четвертого блока обучения, ваша задача заключается в следующем:

- a. Какой модуль **FreePBX** покажет вам на сущность (транк, номер), где установлен слабый пароль?
- b. Какую роль выполняет файл **.rhosts** в работе **SSH**?
- c. Выполните все требования из пройденного урока по безопасности IP - ATC Asterisk. Оставьте открытыми только порты 10 000 - 20 000, 5060, 5061, 443 и 22. Настройте **Firewall** и разрешите IP - адреса LAN и провайдера.