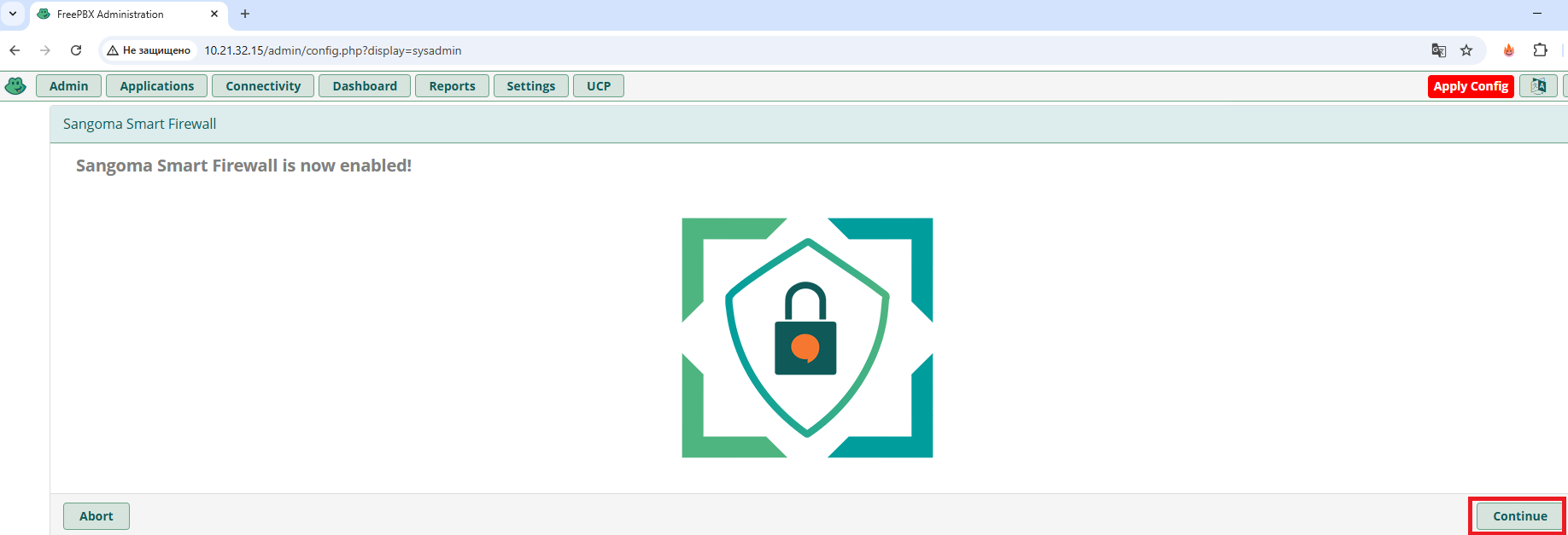
Настройка Firewall в freePBX.

5) Дальше нас поприветствует встроенный Firewall Sangom-ы.

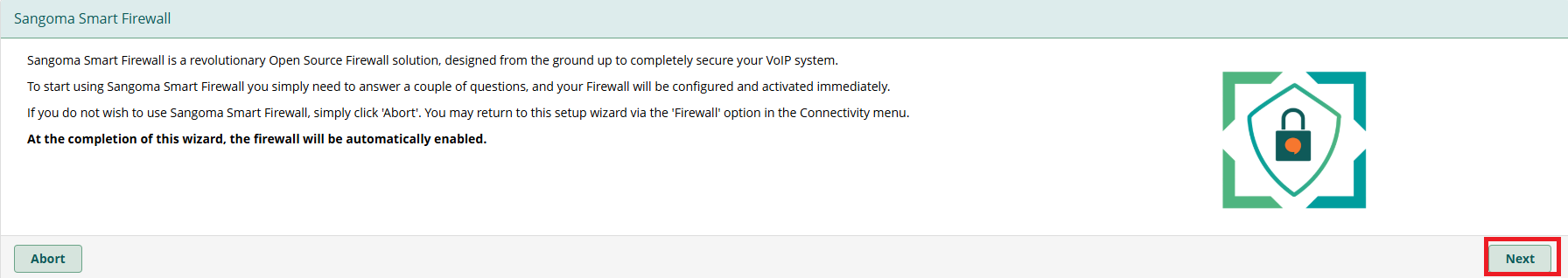
Будут появляться окна вот такого характера:

Порядок данных окон может немного отличаться, но по сути, там везде просто жмём «**Yes**», «**Next**» и «**Continue**».

Здесь жмём «Continue» (Продолжить).

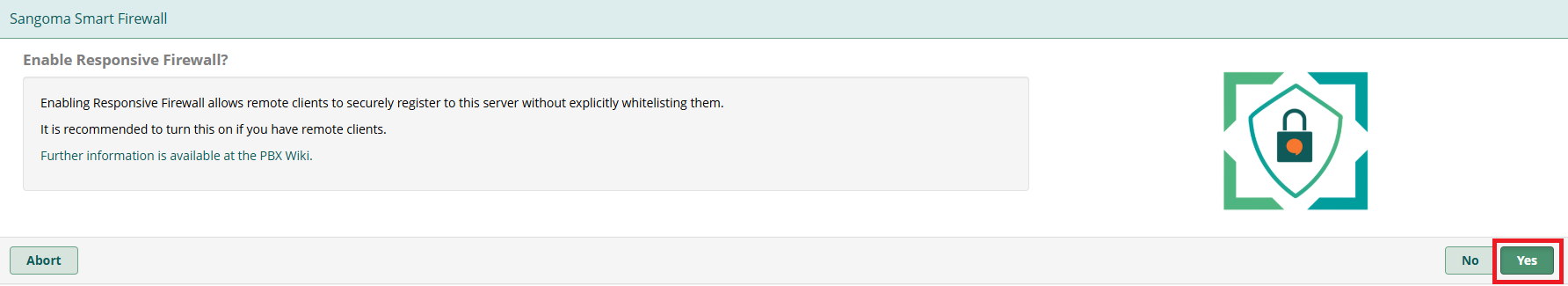


«**Next**» (Далее).



«Включение адаптивного брандмауэра позволяет удалённым клиентам безопасно регистрироваться  
на этом сервере без добавления их в белый список».

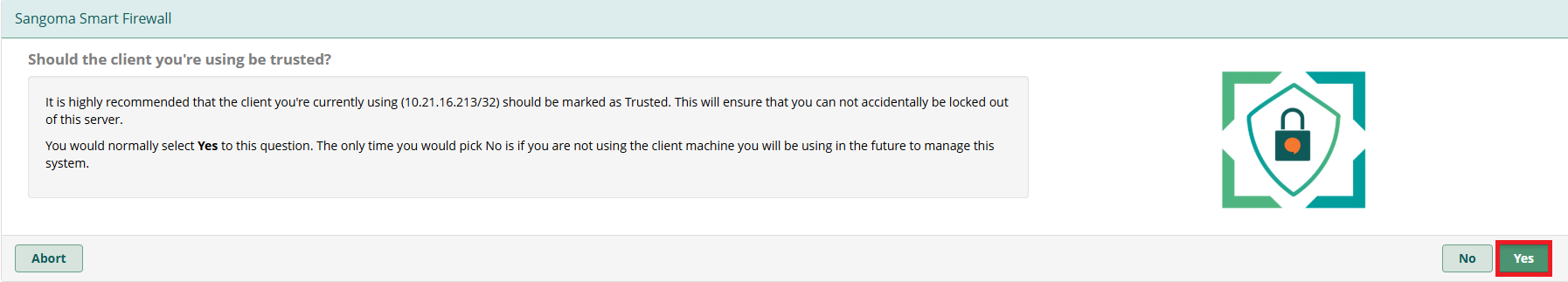
Тут тоже «ДА».



«Настоятельно рекомендуется отметить используемый вами клиент (IP адрес такой-то) как доверенный.  
Это предотвратит случайную блокировку доступа к этому серверу.

Обычно, на этот вопрос отвечают **да**. Ответьте **нет,** если вы НЕ используете клиентский компьютер, который  
будете использовать в будущем для управления этой системой.»

Тут отвечаем «ДА».



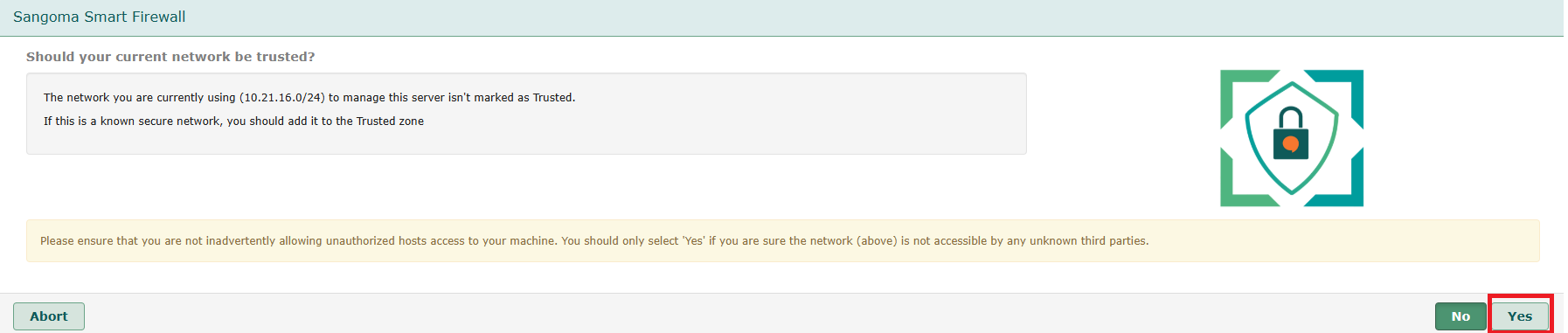
«Сеть, которую вы используете в настоящий момент (Сетка такая-то) для управления этим сервером,

не отмечена как доверенная. Если это известная вам безопасная сеть, добавьте её в доверенную зону.»

«Убедитесь, что вы случайно не предоставляете неавторизованным хостам доступ к своему компьютеру.

Выбирайте «Да» только в том случае, если вы уверены, что сеть (см. выше) недоступна для неизвестных третьих лиц.»

Здесь тоже нажимаем «ДА».



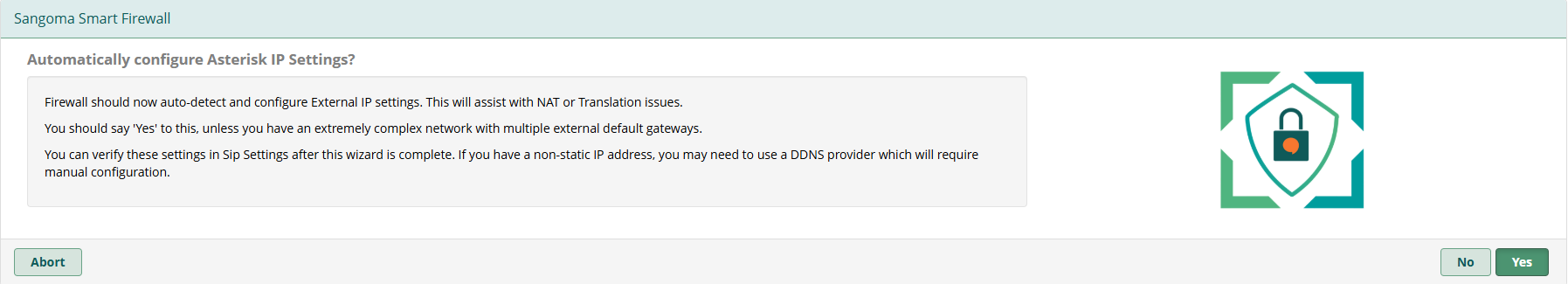
«Теперь брандмауэр должен автоматически определять и настраивать параметры внешнего IP адреса.  
Это решит проблемы с NAT. Следует ответить «ДА», только если у вас не очень сложная сеть с несколькими внешними шлюзами по умолчанию.

Если же у вас сеть не такая, то ответить «ДА» у вас просто не получится и пройти дальше система вам просто не даст.

Вы можете проверить эти параметры в настройках SIP после завершения работы мастера.  
Если у вас НЕ статический IP адрес, вам может понадобиться использовать DDNS от провайдера для чего потребуется ручная настройка.

Здесь, по идее, тоже «ДА», но, если нажать «ДА» не даёт, тогда пока нажимаем «НЕТ» и проходим далее.

После чего нажимаем красную кнопочку «**Apply config**» вверху справа.

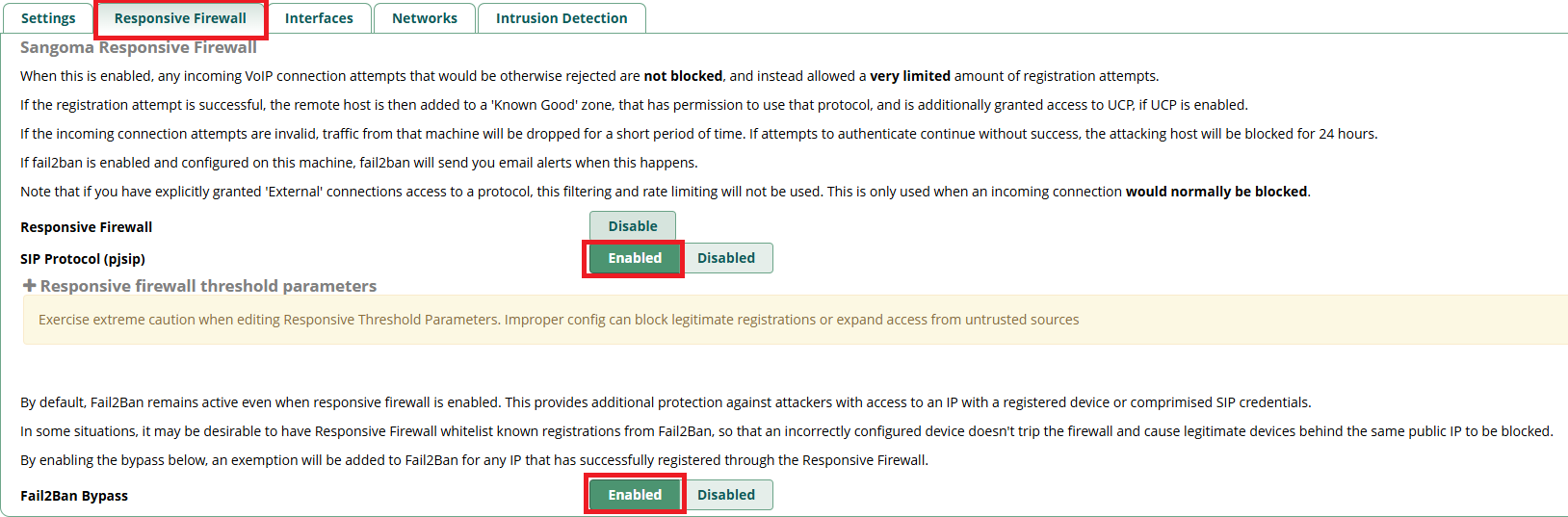


Теперь перейдём к более детальной настройке Firewall-a.

Заходим Connectivity – Firewall.

**Первая вкладка Responsive Firewall**.

Здесь должно быть вот так:



**Responsive Firewall** – это:

При включении этой функции любые входящие попытки VoIP-подключения, которые в противном случае были бы отклонены, не блокируются, а вместо этого разрешается очень ограниченное количество попыток регистрации.

Если попытка регистрации успешна, удаленный хост добавляется в зону «Known Good», которая имеет разрешение на использование этого протокола, и ему дополнительно предоставляется доступ к UCP, если UCP включен.

Если входящие попытки подключения оказываются недействительными, трафик с этого компьютера будет сброшен на короткое время. Если попытки аутентификации продолжатся безуспешно, атакующий хост будет заблокирован на 24 часа.

Если на этом компьютере включен и настроен fail2ban, fail2ban будет отправлять вам уведомления по электронной почте при возникновении подобных ситуаций.

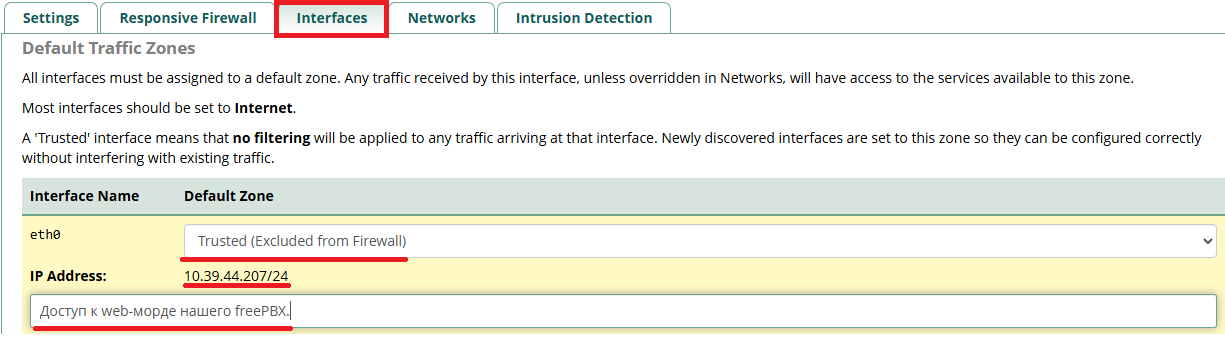
**Fail2Ban Bypass** – это:

По умолчанию Fail2Ban остаётся активным даже при включённом адаптивном брандмауэре. Это обеспечивает дополнительную защиту от злоумышленников, имеющих доступ к IP-адресу с зарегистрированным устройством или скомпрометированных учётных данных SIP.

В некоторых ситуациях может быть желательно, чтобы адаптивный брандмауэр добавлял известные регистрации в Fail2Ban в белый список, чтобы неправильно настроенное устройство не вызывало срабатывание брандмауэра и не приводило к блокировке легитимных устройств с тем же публичным IP-адресом.

При включении обходного пути в Fail2Ban будет добавлено исключение для любого IP-адреса, успешно зарегистрированного через адаптивный брандмауэр.

**Вторая вкладка Interfaces.**

****

*Здесь будет указан наш сетевой интерфейс, т.е. наш IP адрес, через который мы попадаем на веб-интерфейс freePBX и возможность оставить комментарий, что это такое.*

*Если здесь выбрать* ***Internet (Default Firewall)****, то, как только включиться файрволл, мы потеряем доступ к веб-интерфейсу.*

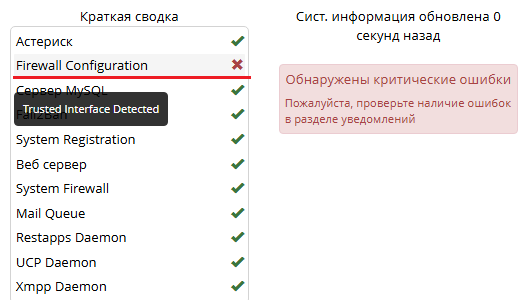
*Так что здесь лучше выбрать либо* ***Trusted (Excluded from Firewall)****, либо* ***Local (Local trusted traffic)****.*

*Таким образом, мы как бы говорим «****полностью доверять данному IP адресу с которым мы работаем****».*

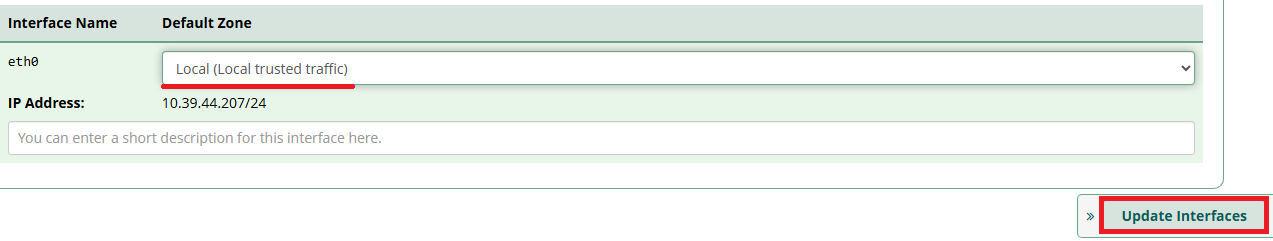
*Таким образом, данный интерфейс будет исключён из Firewall и никак не будет им обрабатываться,*

*соответственно Firewall не будет участвовать в обработке и фильтрации пакетов.*

Что делать, если в дашбоарде freePBX вот такая картина?  
Firewall сообщает нам о том, что у нас есть доверенные (ну, типа «открытые») интерфейсы.



Заходим Connectivity – Firewall – Interfaces и делаем вот так:



То есть, переключаем интерфейс в ***Local (Local trusted traffic).*** *После этого нажимаем «****Update Interfaces****».*

*Затем снова переходим в дашбоард и видим, что всё изумрудно-зелено.*

**Третья вкладка Networks.**

*В сети добавляем наши локальные подсети и промежуточные Firewall-ы, если таковые имеются.*

*В данную вкладку добавляются сети, или хосты которым даётся разрешение по умолчанию.  
Это что-то вроде прероутинга в Микротиках.*

*Таким образом, мы как бы говорим: «Вот этим сетям, или IP адресам доверять 100%, а вот эти обрабатывать файрволлом».*

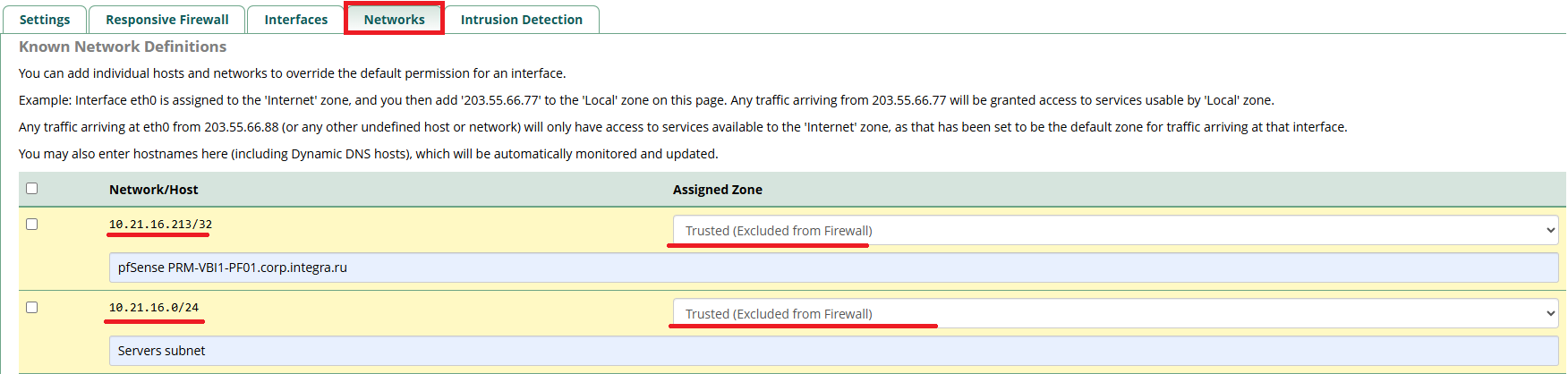
*В данном случае, у нас:*

*10.21.16.213/32 – IP адрес нашего pfSense (софтверный межсетевой экран),*

*10.21.16.0/24 – вся серверная подсеть*

*10.21.32.0/24 – и вся админская подсеть + веб-морда freePBX, которая живёт внутри неё.*

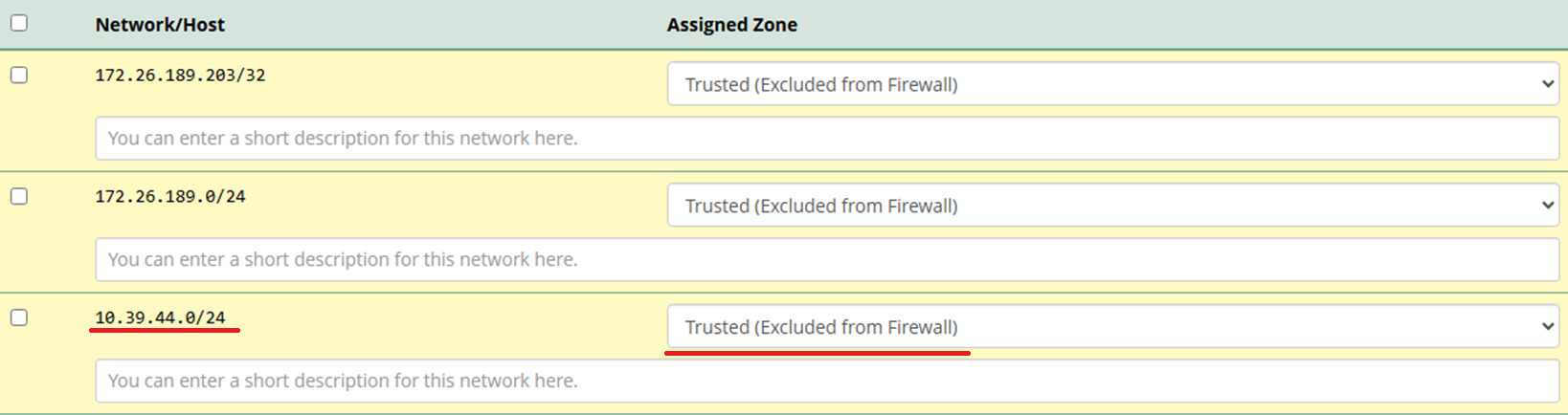
*На скриншоте не отображено, но тоже должно быть* ***Trusted (Excluded from Firewall)***



***Ещё пример сетей.***

*Web-морда открывается по IP-шнику 10.39.44.207, соответственно сеть 10.39.44.0/24 должна быть исключена из Firewall.*

*Если по каким-то причинам не хотите открывать всю сеть 10.39.44.0/24, можно также добавить только один IP-шник 10.39.44.207.  
Это всё та же закладка «****Networks****».*

******

**Четвёртая вкладка Intrusion Detection. О ней чуть более подробно в файле 3.1.**

*В белый лист точно также добавляем все подсети и IP адреса, которым точно можно доверять.*

*В данном случае:*

*127.0.0.1 – это локалхост, т.е. говорим: «доверять самому себе».*

*10.21.16.0/24 – серверная подсеть.*

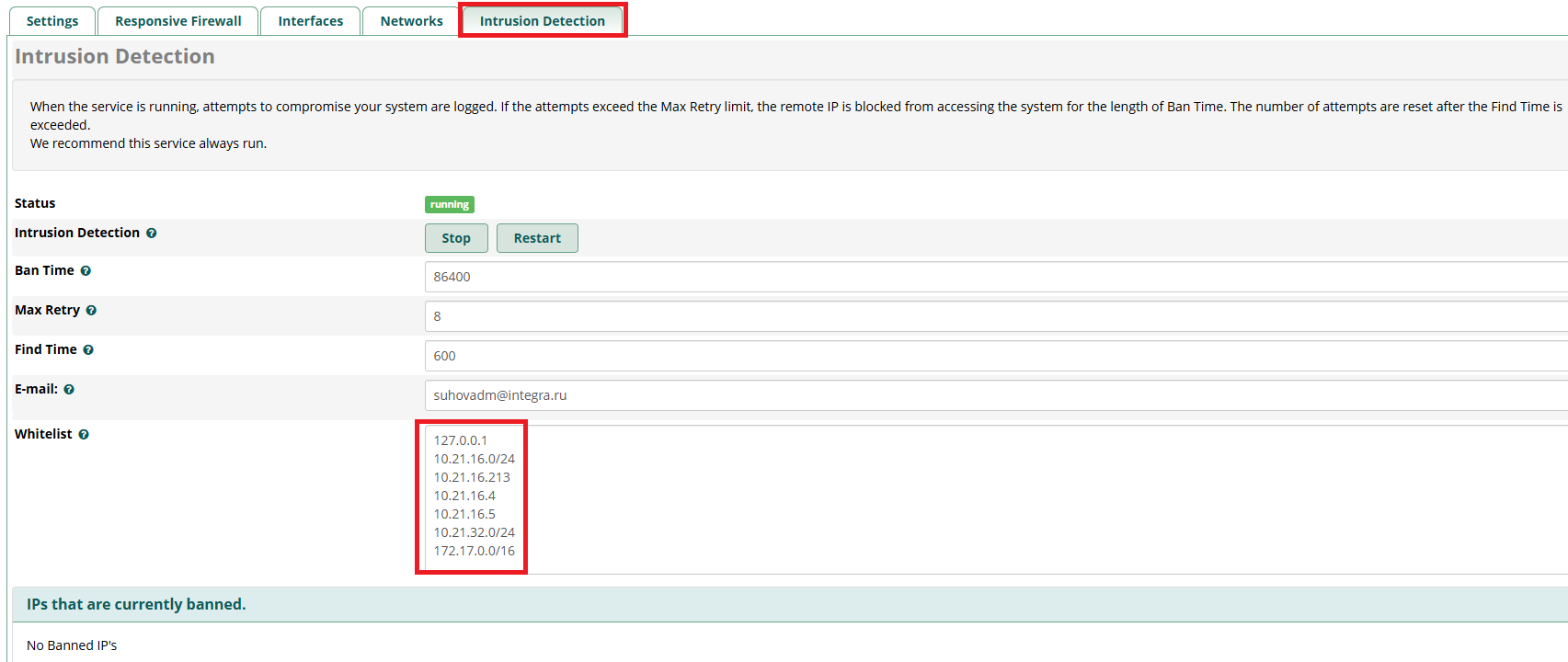
*10.21.16.213 – конкретный адрес межсетевого экрана, в нашем случае это pfSense.*

*10.21.16.4 и 10.21.16.5 – это два локальный кэширующих DNS-а.*

*10.21.32.0/24 – админская подсеть. В ней же живёт веб-морда, через которую открывается freePBX.*

*172.17.0.0/16 – сеть, в которой живут IP телефоны.*

*НАСТРОЙКИ БАН-ТАЙМА ДЕФОЛТНЫЕ, ИХ РАЗБЕРЁМ В СЛЕДУЮЩЕМ ФАЙЛЕ…*

****

*После настройки Firewall, желательно перезапустить Астериск, чтобы убедиться, что всё работает.*