Автор:
02.04.12 09:41 - Последнее обновление 02.04.12 09:53

Руководство по pfSense 2.0. Часть 14

Часть 14 PPTP VPN

оглавление

pfSense может использоваться в качестве сервера VPN PPTP (как один из вариантов организации VPN). Это весьма привлекательная возможность, поскольку клиент PPTP имеется практически в любой версии Windows или OS X выпущенной за последние 10 лет. Кроме того вы можете предоставить услуги по передачи сервиса внутреннему PPTP серверу. Общее обсуждение VPN, доступных в pfSense, их достоинства и недостатки описываются в главе 12 "Виртуальные частные сети".

PPTP предупреждение безопасности

Если вы не использовали PPTP раньше, вам следует обратиться к разделу 12.2.7 "Криптографическая защита" рассказывающему о безопасности VPN. PPTP достаточно широко используется, однако это не самое безопасное решение VPN

PPTP и правила брандмауэра

По умолчанию, когда вы используете перенаправление PPTP или включаете сервер PPTP, для WAN будут автоматически добавлены скрытые правила брандмауэра, разрешающие TCP 1723 и трафик GRE от любого источника до адреса получателя. Вы можете отключить поведение по умолчанию на pfSense 1.2.3 и более поздних версиях отметив чекбокс <Отключить все авто добавления VPN правил> (Disable all auto- added VPN rules) в меню Система >> Дополнительно (System >> Advanced). Вы можете захотеть использовать эту возможность, если точно знаете, что ваши PPTP клиенты будут соединяться только с определённых удалённых сетей. Это позволит предотвратить потенциальные злоупотребления с произвольных узлов, хотя в тех

развертываниях системы, где пользователи мобильны и соединения производятся с различных узлов, знать все подключения невозможно и не практично использовать сжатый набор правил, в итоги приводящий к проблемам пользователей.

PPTP и multi-WAN

К сожалению, из-за способа работы PPTP и способа работы PF с протоколом GRE, возможность запуска PPTP сервера реализована только для основного WAN интерфейса.

Ограничения PPTP

Код отслеживания состояния лежащий в основе брандмауэра PF для протокола GRE позволяет отслеживать только единственную сессию на публичном IP внешнего сервера. Это означает, что если вы используете соединение PPTP VPN, только одна внутренняя машина одновременно может соединиться с PPTP сервером в интернет. Тысяча машин может одновременно соединиться с тысячей различных серверов PPTP, но только одна машина может присоединяться к одному серверу одновременно. Единственная возможность - использовать множество публичных IP на вашем брандмауэре, один на клиент, или использовать множество публичных IP на внешнем PPTP сервере. С другими типами VPN соединений таких проблем нет. Это же ограничение означает, что если вы добавляете функции PPTP сервера или перенаправления PPTP, никакие клиенты подключенные через NAT к вашему WAN IP адресу не смогут соединиться с внешним PPTP сервером. Рабочее решение - доступ клиентов в интернет через NAT реализуется с различных публичных IP адресов. Оба этих ограничения позволяют работу в большинстве сред, однако их устранение имеет высокий приоритет для релиза pfSense 2.0. Во время написания этой книги, ведутся разработки позволяющие устранить эти ограничения, хотя говорить о их успехе пока ещё рано.

Конфигурирование сервера PPTP

Для конфигурирования PPTP сервера, перейдите в меню VPN >> PPTP. Выберите Включить PPTPсервер (EnablePPTPserver).

Вам необходимо решить, какие IP адреса использовать для сервера PPTP и клиентов. Обычно, удалённое пространство адресов - часть подсети LAN например такой как 192.168.1.103. Затем вам следует выбрать IP адрес за пределами данного диапазона для адреса сервера, например 192.168.1.244, как показано на рисунке 14.1, "IP адресация PPTP".

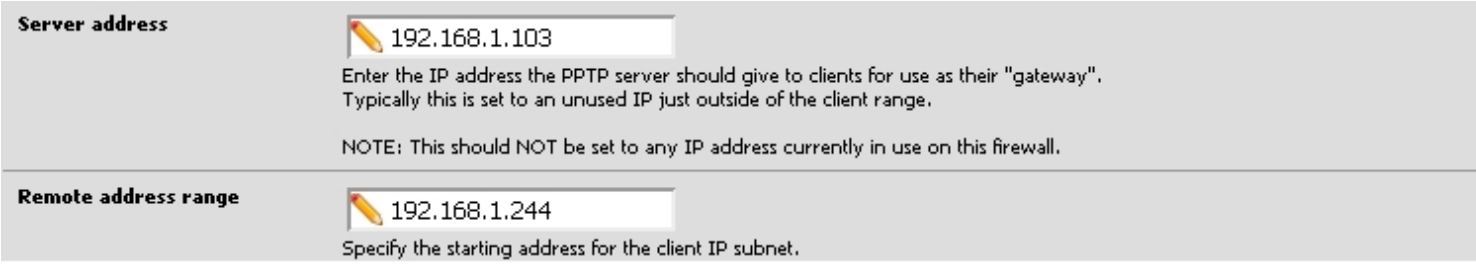

Рис.14.1 IP адресация PPTP

NOTE: Эта подсеть может не входить в пределы существующей подсети вашего маршрутизатора. При желании вы можете использовать различный набор IP адресов.

Аутентификация

Можно производить аутентификацию пользователей по локальной базе пользователей, или посредством RADIUS-сервера. RADIUS позволяет соединяться с другим сервером в вашей сети, для целей аутентификации. Такая возможность может использоваться для аутентификации пользователей PPTP с помощью Microsoft Active Directory (см. раздел 24.1 "Аутентификация RADIUS с Windows Server"), или другими RADIUS совместимыми серверами. Для использования RADIUS, установите флаг <Использовать сервер RADIUS> (Use a RADIUS server) и заполните поля во вкладках и . Для аутентификации с использованием локальной базы данных пользователей, снимите данный флаг. Если вы используете RADIUS вам не нужно вам не нужно добавлять пользователей на вкладке Users VPN >> PPTP. Смотрите раздел 14.5.6, "Добавление пользователей" более подробно рассматривающий встроенную систему аутентификации.

Необходимость 128 битного шифрования

Используйте 128 битное шифрование везде где это возможно. Большинство клиентов PPTP поддерживают 128 битное шифрование, таким образом, оно прекрасно работает в большинстве сетевых сред. PPTP достаточно слабо защищён даже при использовании 128 битного шифрования и тем более при 40 и 56 битном. Если специальных требований нет, недопустимо использовать шифрование ниже чем 128 бит для PPTP.

После заполнения вышеописанных настроек, нажмите Save. При этом ваша конфигурация будет сохранена и PPTP сервер запустится. Если вы аутентифицируете своих пользователей по локальной базе, перейдите на вкладку Users и введите данные своих пользователей.

Открываем Firewall >> Rules и выбираем закладку PPTP VPN. Эти правила управляют трафиком клиентов PPTP. Пока вы не добавите правила брандмауэра, весь трафик инициируемый клиентами PPTP будет блокироваться. Трафиком исходящим от внутреннего LAN до клиентов PPTP управляют правила брандмауэра LAN. Для начала можно добавить правило разрешающие весь трафик, как показано на рисунке 14.2, "Правила

брандмауэра VPN PPTP", но после тестирования работы следует ввести более жёсткие

ограничения на данные правила.

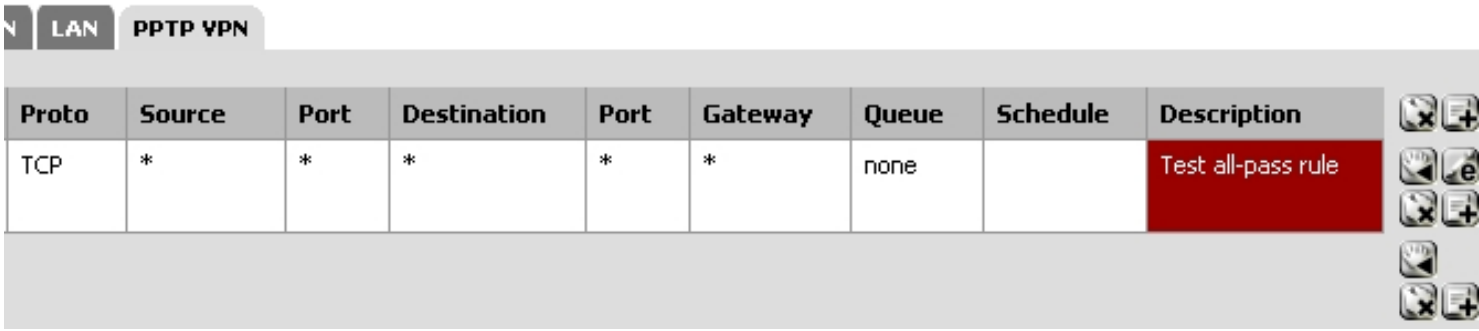

Рисунок 14.2

Добавление пользователей

Добавление пользователей для сервера RADIUS может меняться от версии к версии. Эта процедура выходит за рамки контекста этого раздела, и рассматривается в документации на RADIUS сервер. Добавление пользователей во встроенную базу pfSense производится достаточно просто. Во-первых, выберите VPN >> PPTP и перейдите на вкладку Users. Вы увидите пустую таблицу пользователей показанную на рисунке 14.3, "Вкладка Пользователи PPTP". Нажмите кнопку для добавления пользователя.

Рисунок 14.3

После нажатия иконки [+] появится страница редактирования пользователя. Заполните имя и пароль пользователя как показано на рисунке 14.4 "Добавление пользователя PPTP". При желании можно ввести статический IP присваиваемый пользователю.

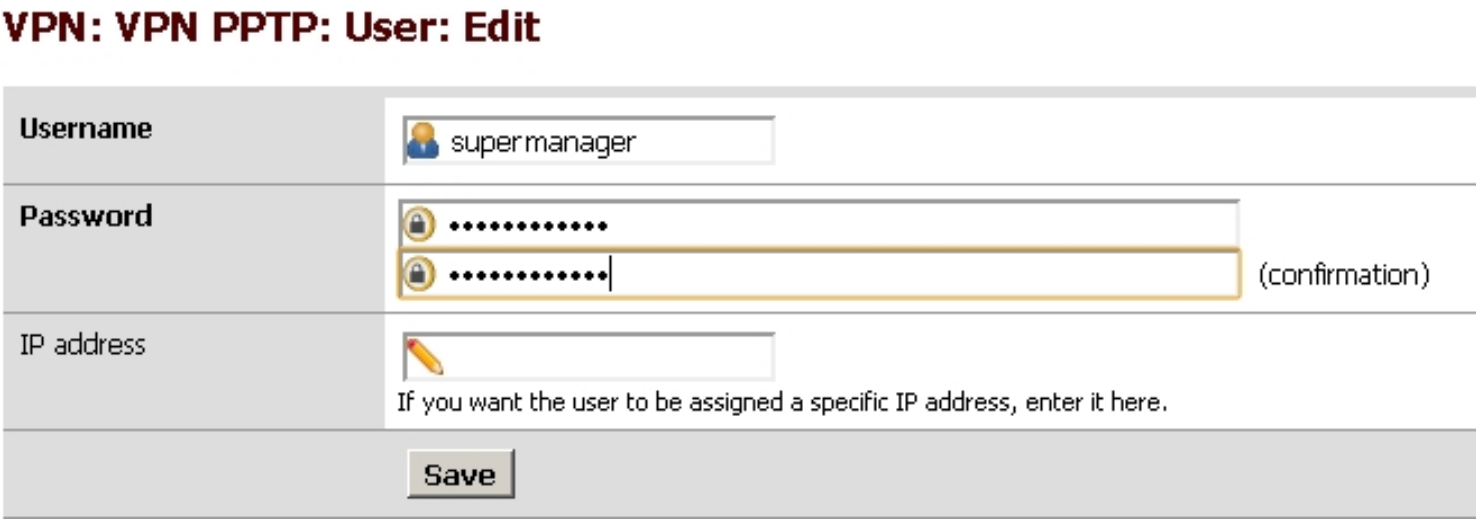

Рисунок 14.4

Нажмите Save и вы вернётесь на страницу списка пользователей (рисунок 14.5 "Применение параметров PPTP"), и нажмите кнопку Apply Changes для применения изменений.

VPN: VPN PPTP: Users

The PPTP user list has been modified.
You must apply the changes in order for them to take effect.
Warning: this will terminate all current PPTP sessions!

Apply change

Configuration | Users

Username	IP address
supermanager	

Рисунок 14.5 [illegible] "Вид [illegible] PPTP"

VPN: VPN PPTP: Users

The PPTP user list has been modified.
You must apply the changes in order for them to take effect.
Warning: this will terminate all current PPTP sessions!

Apply

Configuration | Users

Username	IP address
supermanager	
salesguy	192.168.1.176
user	

Рисунок 14.6 [illegible]

Last 150 PPTP VPN log entries

Time	Action	User	IP address
Jul 17 12:46:26	◀	rick	
Jul 17 12:08:52	▶	rick	192.168.130.128

Рисунок 14.35 [illegible] "Журнал PPTP", [illegible] IP