Автор:
02.04.12 11:38 - Последнее обновление 02.04.12 14:42

Руководство по pfSense 2.0. Часть 7

Часть 7 Трансляция сетевых адресов (NAT)

оглавление

В наиболее общем смысле, NAT (Network Address Translation) позволяет подключить несколько компьютеров к сети Интернет, используя единственный внешний IP адрес. pfSense реализуют данный функционал в базовом развёртывании, а кроме того имеет возможности более расширенного и сложного конфигурирования NAT необходимого в сетях с несколькими публичными IP адресами. NAT настраивается в двух направлениях - входящем и исходящем. Исходящий NAT определяет работу с трафиком исходящим из сети в сеть Интернет. Входящий NAT работает с трафиком входящим в вашу сеть из Интернет. Наиболее распространённый тип входящего NAT, и один из наиболее знакомых, называется форвардингом портов.

7.1. Конфигурация NAT по умолчанию.

В данном разделе описывается конфигурация NAT используемая в pfSense по умолчанию. Чаще всего подходящая конфигурация NAT генерируется автоматически. В некоторых средах вы можете захотеть изменить эту конфигурацию и pfSense позволяет сделать это в полном объёме посредством Web-интерфейса. Это выгодно отличает pfSense от прочих брандмауэров проекта Open Source.

7.1.1. Конфигурация исходящего NAT по умолчанию.

Конфигурация NAT по умолчанию, используемая в pfSense с интерфейсами LAN и WAN автоматически транслирует интернет трафик в WAN IP адреса. Когда настроены несколько WAN интерфейсов, трафик покидающий любой WAN интерфейс автоматически транслируется в адрес используемого WAN интерфейса. Статический порт автоматически настраивается для трафика IKE (часть IPSec) и SIP(VoIP). Статический порт более подробно будет рассмотрен в разделе 7.6, "Исходящий NAT".

7.1.2. Конфигурация по умолчанию для входящего NAT

По умолчанию, никакой трафик из Интернет внутрь не допускается. Если вам

требуется позволить трафику инициированному в Интернет попадать в вашу внутреннюю сеть, вы должны настроить форвардинг портов или 1:1 NAT. Эти возможности мы рассмотрим в следующих разделах.

7.2. Порт форвардинг (Port Forwards)

Порт-форвардинг (или если угодно перенаправление портов) позволяет вам открыть специфичный порт, диапазон портов или протокол для приватных адресов устройств в вашей сети. Название "port forward" было выбрано после бесчисленного числа жалоб. Однако этот термин не совсем верен, поскольку вы можете перенаправить GRE и ESP протоколы в дополнение к портам TCP и UDP. Наиболее часто это используется при хостинге серверов или использовании приложений, которые требуют входящего соединения из Интернет.

7.2.1. Риски использования форвардинга портов

В конфигурации по умолчанию, pfSense не позволяет любой трафик инициированный в Интернет. Это обеспечивает защиту от любого сканирования системы при поисках целей атаки. При включении форвардинга портов, pfSense позволяет любой трафик соответствующий правилу брандмауэра. Система не разбирается в типе пропускаемого пакета. Если он удовлетворяет правилу - он разрешён. В данном случае, вам придётся полагаться на систему безопасности конечного хоста.

7.2.2. Перенаправление портов и локальные сервисы

Порт-форвардинг может быть запущен относительно любой службы работающей локально на брандмауэре, например web интерфейсу, SSH и прочим запущенным сервисам. Например, это означает, что если вы позволили удалённый доступ с WAN используя HTTPS на порт TCP 443, если вы добавили перенаправление порта на WAN для TCP 443, то стандартный доступ к web интерфейсу работать не будет. Это не повлияет на доступ к другим интерфейсам.

7.2.3. Добавление перенаправления портов

Перенаправление портов управляется в меню Firewall -> NAT, на закладке Port Forward. Правила на этом экране управляются аналогично правилам брандмауэра (смотрите раздел 6.2. "Введение в экран правила брандмауэра").

Для начала добавления перенаправления порта, нажмите кнопку [+] в верхней или нижней части списка, как показано на рисунке 7.1 "Добавление перенаправления порта".

Рисунок 7.1 "Добавление перенаправления порта"

Теперь, вы должны увидеть экран редактирования перенаправления порта, показанный на рисунке 7.2. "Пример перенаправления порта", с параметрами выбранными по умолчанию. Во-первых, выберите интерфейс (Interface), на котором будет находится перенаправляемый порт. В большинстве случаев это будет WAN, однако, если у вас есть интерфейс OPT, или если используется локальное перенаправление, это может быть другой интерфейс. Внешний адрес (External Address), в большинстве случаев, должен быть установлен в адрес интерфейса или доступный виртуальный IP (смотрите раздел 6.8. "Виртуальные IP"), если это локальное перенаправление. Протокол (Protocol) и диапазон внешних портов (External Port Range) должны быть установлены в соответствии с перенаправляемой службой. Например, для перенаправления VNC1 в должны установить протокол в значение TCP, а диапазон внешних портов в значение 5900. (Поскольку это стандартно перенаправляемый порт, он так же доступен в списке выпадающего меню выбираемых портов.)
NAT IP должен быть установлен в локальный IP адрес, по которому перенаправляется данный порт, а локальный порт (Local Port) - в значение начала диапазона перенаправляемых портов. Если вы перенаправляете диапазон портов, скажем 19000-19100, вам необходимо указать локальную начальную точку, поскольку порты должны соответствовать по принципу "один к одному". Это поле позволяет открывать порт на внешней стороне, отличающийся от того на котором слушает внутренний хост, например, внешний порт 8888 может перенаправляться на локальный порт 80 внутреннего HTTP сервера. Поле Описание (Description), как и в других местах pfSense, доступно для внесение краткой информации о назначении создания перенаправления.
Если вы не используете отказоустойчивый кластер CARP, пропустите опцию XML-RPC Sync. Если это не так, этот флаг будет препятствовать синхронизации данного правила с другими членами отказоустойчивого кластера (смотрите главу 20, "Избыточность брандмауэра/ Высокая доступность"), что обычно не желательно.

Последняя опция является очень важной. Если вы отметите Auto-add a firewall rule to permit traffic through this NAT rule (Добавлять правило брандмауэра автоматически, чтобы разрешить трафик через это правило NAT), то правило брандмауэра, для вас, будет создано автоматически, и это позволит трафику добраться до порта назначения. Как правило, лучше оставить эту опцию отмеченной, а позже, при необходимости, изменить правило брандмауэра.

Нажмите кнопку Save (Сохранить), по завершению конфигурирования, а затем Apply Changes (Применить изменения). На рисунке 7.2 "Пример перенаправления порта", показан пример экрана редактирования перенаправления порта, заполненный настройками для перенаправления VNC в локальную систему.

Автор:
02.04.12 11:38 - Последнее обновление 02.04.12 14:42

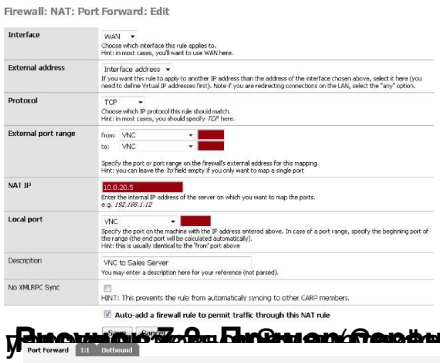
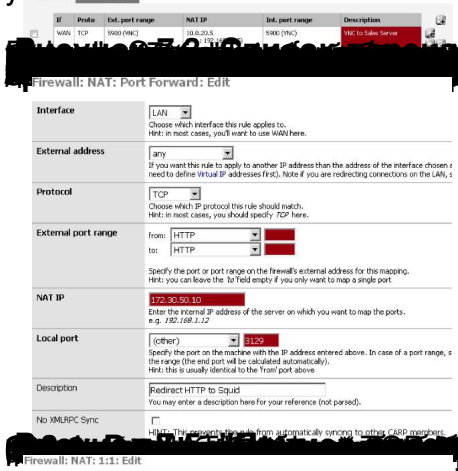
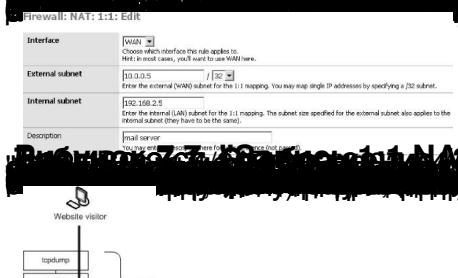
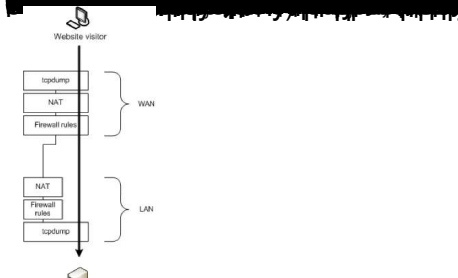


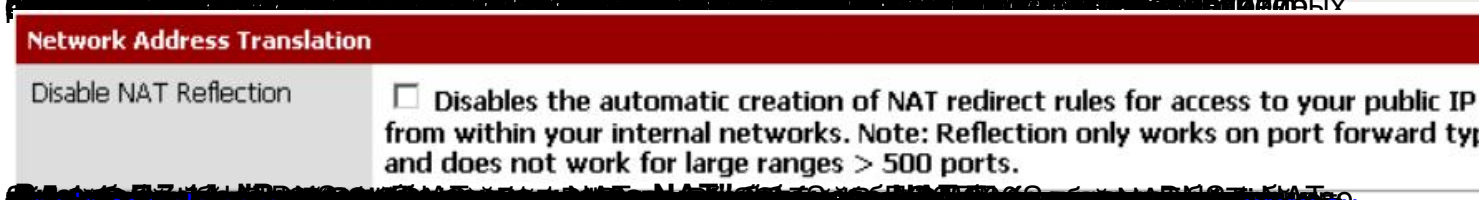
Рисунок 7.9. Проброс/перенаправление порта







TCP	*	*	192.168.1.5	80 (HTTP)	*		NAT forw



Автор:
02.04.12 11:38 - Последнее обновление 02.04.12 14:42