Автор: Administrator
27.03.12 08:46 - Последнее обновление 28.06.12 11:16

Выборочная переадресация HTTP запросов на веб страничку

в PfSense 2.0 средствами vHosts

Установка, настройка пакета vHosts в PfSense 2.0

"Требуется все запросы от всех адресов дефолтно перенаправлять на отдельный веб-сервер (на его 80 й порт). По сути, все не учтенные ип-адреса при любом запросе должны попадать только туда."

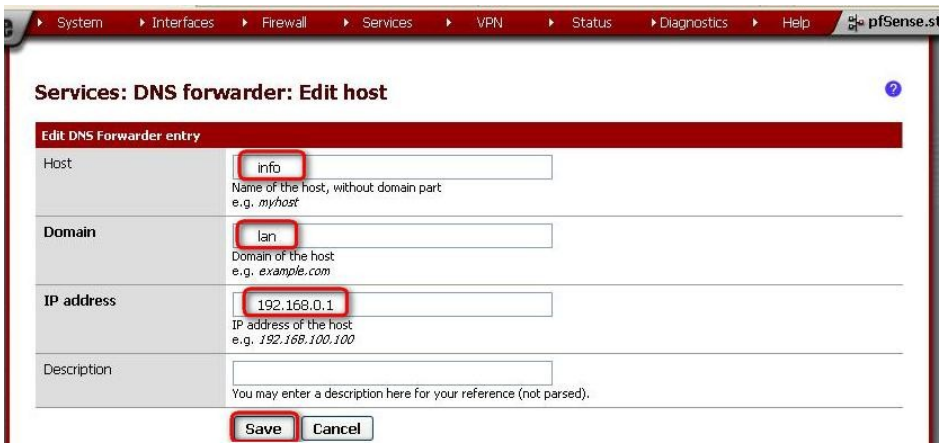
Перефразирую:
Мы создадим список IP адресов пользователей, которые смогут выходить в интернет. Все остальные IP адреса из локальной сети, будут попадать на информ страничку. Данный функционал чаще нужен провайдерам интернет. В случае отсутствия абанплаты, удаляем IP из списка и всё HTTP запросы будут отправляться на информационную веб. страничку.

Подразумевается, что у вас PfSense с начальными настройками - реквизиты интерфейсов, DNS, DHCP, NAT. Всё настроено и вы можете выходить через PfSense в интернет.

LAN 192.168.0.1/24

1. Делаем запись в DNS для виртуального хоста (info.lan = 192.168.0.1)

Services -> DNS forwarder



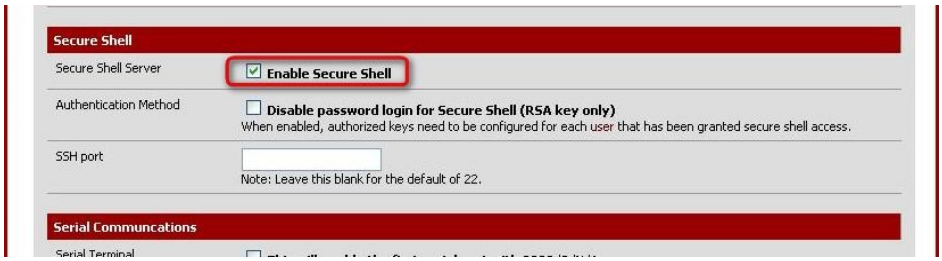
2. С локального компа делаем - ping info.lan

Обмен пакетами с info.lan [192.168.0.1] по 32 байт:

Ответ от 192.168.0.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=64

3. Изменим порт админки и включим SSH доступ.

System -> Advanced

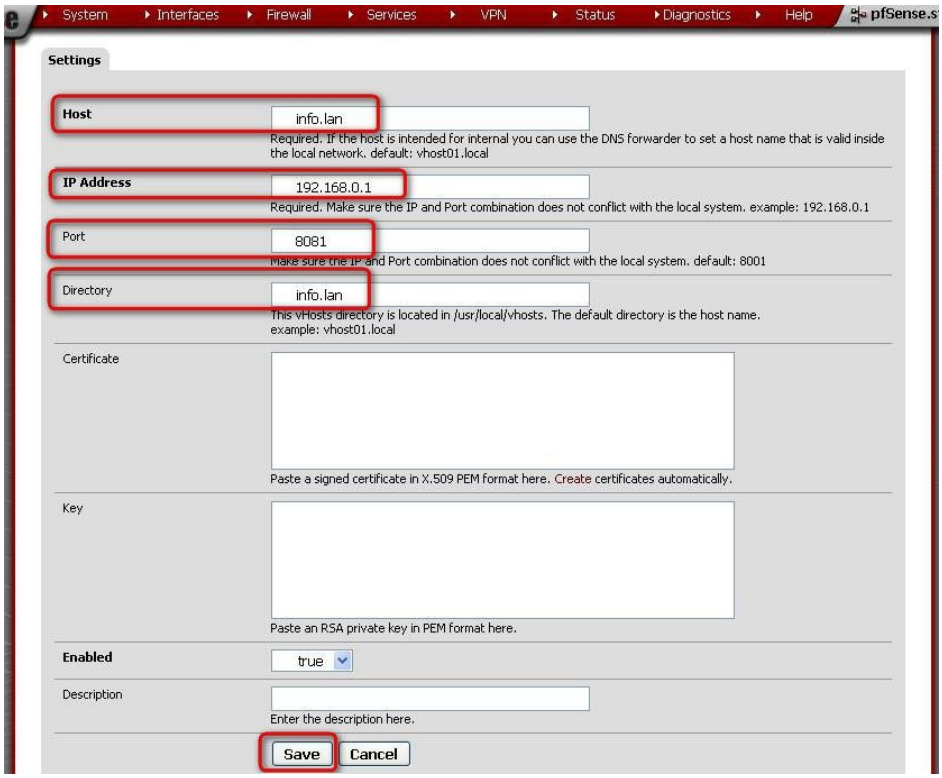


4. Устанавливаем vHosts

System -> Package Manager -> Available Packages

5. Настраиваем vHosts

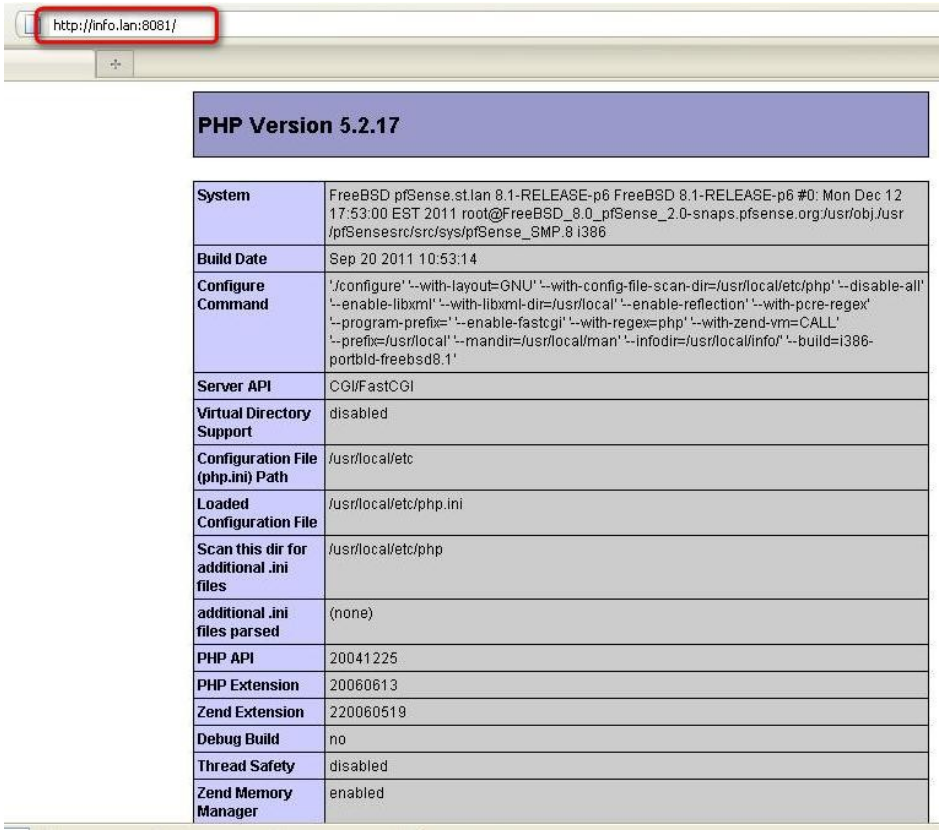
Services -> vHosts



6. Проверяем работу vHosts

Заходим на http://info.lan:8081

Видим:



7. Делаем потрфоравард 80 порт <-> 8081

Firewall -> NAT -> Port Forward

System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help | pfSense.st

Firewall: NAT: Port Forward: Edit

Edit Redirect entry

Disabled	☐ **Disable this rule** Set this option to disable this rule without removing it from the list.
No RDR (NOT)	☐ Enabling this option will disable redirection for traffic matching this rule. Hint: this option is rarely needed, don't use this unless you know what you're doing.
Interface	LAN Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	TCP Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	☐ **not** Use this option to invert the sense of the match. Type: LAN subnet Address: / 31
Source port range	from: any to: any Specify the source port or port range for this rule. **This is usually *random* and almost never equal to the destination port range (and should usually be 'any').** Hint: you can leave the *'to'* field empty if you only want to filter a single port.
Destination	☐ **not** Use this option to invert the sense of the match. Type: any Address: / 31
Destination port range	from: HTTP to: HTTP Specify the port or port range for the destination of the packet for this mapping. Hint: you can leave the *'to'* field empty if you only want to map a single port
Redirect target IP	192.168.0.1 Enter the internal IP address of the server on which you want to map the ports. e.g. *192.168.1.12*

Redirect target port	(other) 8081 Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above
Description	You may enter a description here for your reference (not parsed).
No XMLRPC Sync	☐ HINT: This prevents the rule from automatically syncing to other CARP members.
NAT reflection	use system default
Filter rule association	Rule NAT View the filter rule

Save | Cancel

8. Проверяем работу портфорвардинга

Проверяем правило в **command prompt**

pfctl -sa | grep rdr

Заходим на http://info.lan

Видим картинку пункт 6.

Если не увидели:

Очистить кэш броузера.

Рестарт DNS и vHosts (Status: Services)

Можно и Status: Filter Reload Status

9. Создаем php страничку info.php **с желаемым содержимым**

/usr/local/www/info.php

10. Учим vHosts пускать нас по ip адресу (а не по доменному имени) на нашу веб страничку info.php

Правим /var/etc/vhosts-http.conf

Находим:

```
## a static document-root, for virtual-hosting take look at the
## server.virtual-* options
server.document-root        = "/usr/local/vhosts/"
```

Меняем на: server.document-root = "/usr/local/www"

Находим:

```
        $SERVER["socket"] == "192.168.0.1:8081" {
 $HTTP["host"] == "info.lan" {
 server.document-root        = "/usr/local/vhosts/info.lan"

 }
}
```

Меняем на:

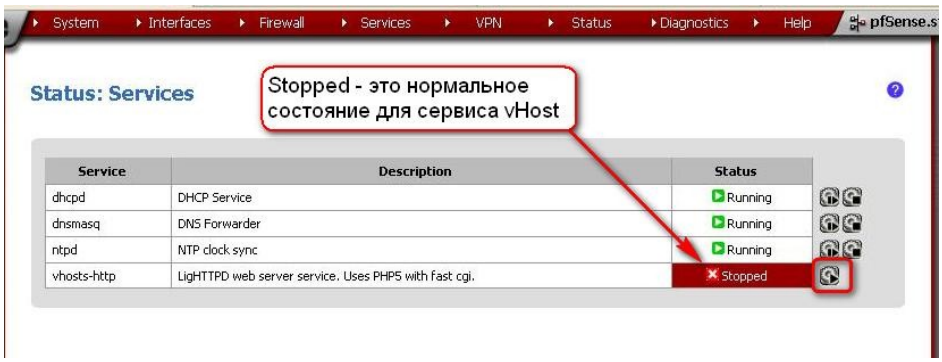
```
$SERVER["socket"] == "192.168.0.1:8081" {
 $HTTP["host"] == "info.lan" {                          #находим имя созданного ранее хоста
 server.document-root        = "/usr/local/www"        #меняем тут папку на указанную

 }
}
```

```
url.rewrite-once  = ("^/(.*)$" => "/info.php")          #эта регулярка позволит нам по любому адресу попадать на указанную
```

После внесённых изменений, рестартуем сервис **vHosts**

Status -> Services



Для того чтобы vhosts-http.conf не был изменен после перезагрузки, делаем

chflags uchange /var/etc/vhosts-http.conf

Для снятия флага, используем команду chflags nouchange /var/etc/vhosts-http.conf

11. С этого момента, все запросы в интернет по 80 му порту, должны переадресовываться на инфо страничку info.php

Проверяем возможность захода по IP адресу

http://192.168.0.1:8081

http://192.168.0.1

12. Создаем Aliases с группой IP адресов, которые смогут выходить в интернет.

Firewall -> Aliases

System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help | pfSense.s

Firewall: Aliases: Edit

Alias Edit

Name: aliace
The name of the alias may only consist of the characters "a-z, A-Z and 0-9".

Description: aliace
You may enter a description here for your reference (not parsed).

Type: Host(s)

Host(s): Enter as many hosts as you would like. Hosts must be specified by their IP address.

IP	Description
192.168.0.99	99
192.168.0.100	100

Save | Cancel

13. Добавляем Port Forward по портфорвардинга

System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help | pfSense.st

Firewall: NAT: Port Forward

Port Forward | 1:1 | Outbound

If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
LAN	TCP	LAN net	*	*	80 (HTTP)	192.168.0.1	8081	

не путаем плюсики!

pass
linked rule

System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help | pfSense.s

Firewall: NAT: Port Forward: Edit

Edit Redirect entry

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

No RDR (NOT): Enabling this option will disable redirection for traffic matching this rule.
Hint: this option is rarely needed, don't use this unless you know what you're doing.

Interface: LAN
Choose which interface this rule applies to.
Hint: in most cases, you'll want to use WAN here.

Protocol: TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify *TCP* here.

Source: not
Use this option to invert the sense of the match.
Type: Single host or alias
Address: aliace / 31

Source port range: from: any, to: any
Specify the source port or port range for this rule. **This is usually *random* and almost never equal to the destination port range (and should usually be 'any').**
Hint: you can leave the *to'*field empty if you only want to filter a single port.

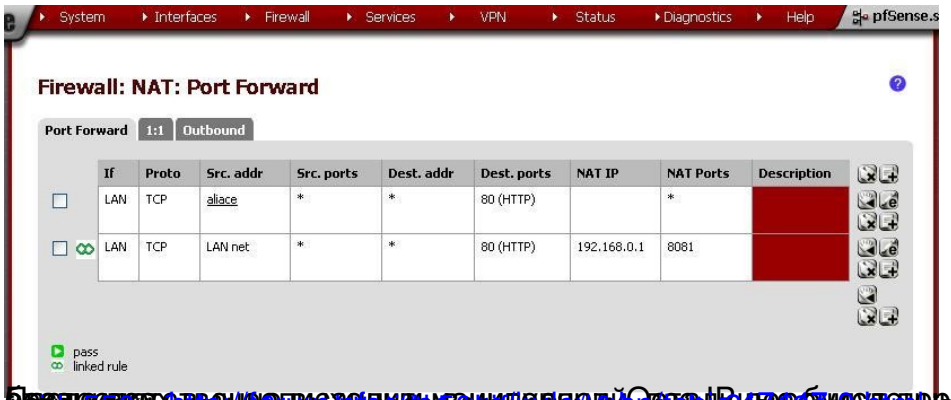
Destination: not
Use this option to invert the sense of the match.
Type: any
Address: / 31

Destination port range: from: HTTP, to: HTTP
Specify the port or port range for the destination of the packet for this mapping.
Hint: you can leave the *to'*field empty if you only want to map a single port

Description:
You may enter a description here for your reference (not parsed).

Перемещаем созданное правило, выше ранее созданного правила в пункте 7.

Автор: Administrator
27.03.12 08:46 - Последнее обновление 28.06.12 11:16



[illegible] IP [illegible] http://www.thin.kiev.ua/index.php?option=com_content&view=article&am