

Автор:

15.10.12 13:32 - Последнее обновление 15.10.12 20:44

Данная статья посвящена настройке PPTP клиента на WAN интерфейсе PfSense 2.0 (WAN статический)

Попытка воспользоваться стандартным wizard в PfSense 2.0 для настройки PPTP клиента на WAN была безуспешна. PPTP клиент упорно не желал подключаться к виндовому (win 2003) серверу. На [форуме](#) получил лекарство от [vardan](#)

Необходимо исправить в /etc/inc/interfaces.inc то что выделено красным цветом

```
        if (!isset($ppp['verbose_log']))
$mpdconf .= <<<EOD
set bundle enable compression
set ccp yes mppc
set mppc yes e40 e56 e128 stateless

#log -bund -ccp -chat -iface -ipcp -lcp -link

EOD;
foreach($ports as $pid => $port){
$port = get_real_interface($port);
$mpdconf .= <<<EOD

create link static {$interface}_link{$pid} {$type}
set link action bundle {$interface}
set link {$multilink} multilink
set link keep-alive 10 60
set link max-redial 0

EOD;
if (isset($ppp['shortseq']))
$mpdconf .= <<<EOD
set link no shortseq

EOD;
```

Автор:

15.10.12 13:32 - Последнее обновление 15.10.12 20:44

```
if (isset($ppp['acfcomp']))
$mpdconf .= <<<EOD
set link no acfcomp
```

EOD;

```
if (isset($ppp['protocomp']))
$mpdconf .= <<<EOD
set link no protocomp
```

EOD;

```
$mpdconf .= <<<EOD
set link disable chap pap
set link accept chap pap eap chap-msv2
set mppc yes compress
set link disable incoming
```

EOD;

```
if (!empty($bandwidths[$pid]))
$mpdconf .= <<<EOD
set link bandwidth {$bandwidths[$pid]}
```

После внесения изменений в interfaces.inc, подключение произошло.

Далее я расскажу как настроить PPTP клиент и "пустить" через PPTP туннель весь трафик.

Исходные данные:

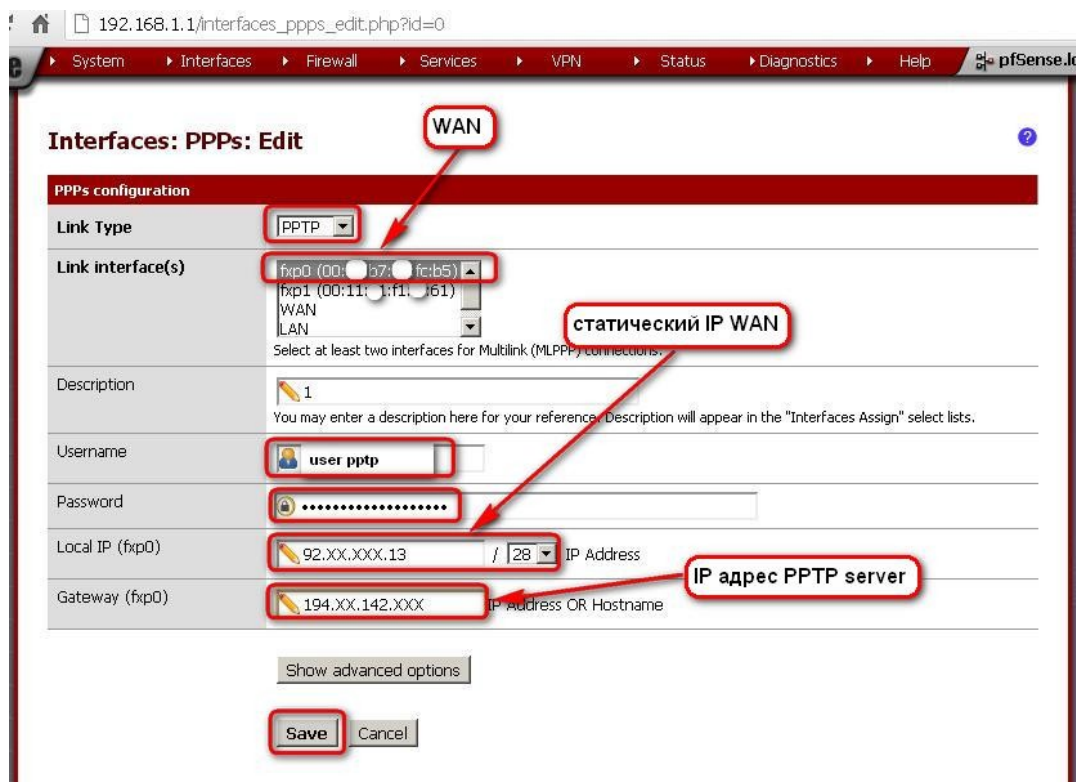
WAN 92.xx.xxx.13/28

LAN 192.168.1.1/24

1. Был запущен мастер (wizard), пройдены все шаги и на выходе получили выход в интернет бер PPTP клиента.

2. Настроим PPTP client

Interfaces -> Assign -> PPPs

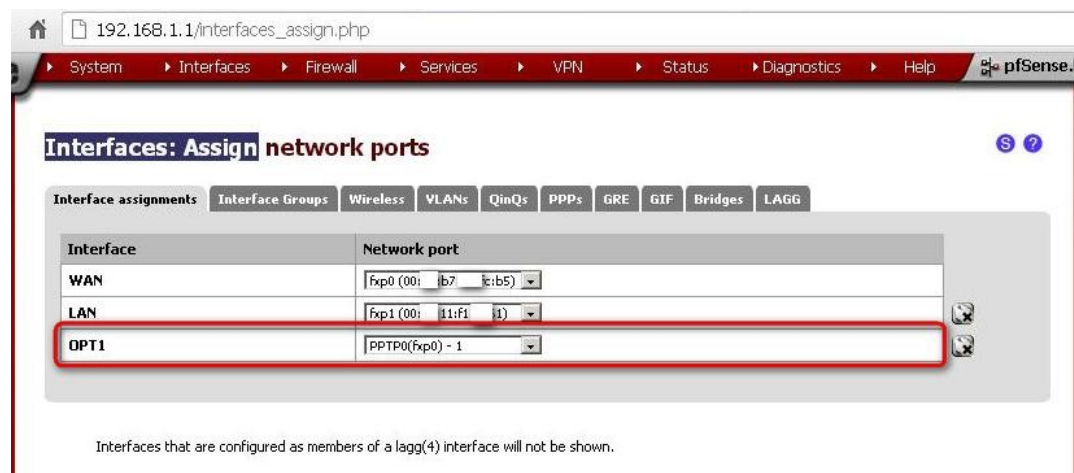


Автор:

15.10.12 13:32 - Последнее обновление 15.10.12 20:44

3. После создания PPTP соединения, у нас появится возможность добавить новый интерфейс OPT1

Interfaces -> Assign -> +



4. Включаем интерфейс OPT1

Автор:

15.10.12 13:32 - Последнее обновление 15.10.12 20:44

General configuration

Enable **Enable Interface**

Description
Enter a description (name) for the interface here.

Type

MAC address
Insert my local MAC address
This field can be used to modify ("spooF") the MAC address of this interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.

MSS
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

PPTP/L2TP configuration

Username

Password

Local IP address /

Remote IP address

Dial on demand **Enable Dial-On-Demand mode**
This option causes the interface to operate in dial-on-demand mode, allowing you to have a *virtual full time* connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

Idle timeout seconds
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

Advanced [Click here for additional PPTP and L2TP configuration options. Save first if you made changes.](#)

Private networks

Block private networks
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8,

5. Убедимся, что все компьютеры появились. Возможно придется "ребутнуть" PfSense

Status: Dashboard

System Information

Name	pfSense.localdomain
Version	2.0.1-RELEASE (386) built on Mon Dec 12 17:53:52 EST 2011 FreeBSD 8.1-RELEASE-p6

Interfaces

WAN	↑ 92 . 13	100baseTX <full-duplex>
LAN	↑ 192.168.1.1	100baseTX <full-duplex>
OPT1	↑ 10.0.127.17	

Видеть роутер по LAN на всех экранах OPT1 (PPTP client)

Автор:

15.10.12 13:32 - Последнее обновление 15.10.12 20:44

The screenshot shows the 'Firewall: Rules: Edit' page in pfSense. The main configuration area includes:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** LAN
- Protocol:** any
- Source:** not, Type: LAN subnet, Address: /
- Destination:** not, Type: any, Address: /
- Log:** Log packets that are handled by this rule
- Description:** Default allow LAN to any rule

Below the main configuration, there is a 'Log' section with a description and 'Save' and 'Cancel' buttons.

The 'Advanced features' section includes:

- Source OS: Advanced - Show advanced option
- Diffserv Code Point: Advanced - Show advanced option
- Advanced Options: Advanced - Show advanced option
- State Type: Advanced - Show advanced option
- No XMLRPC Sync: Advanced - Show advanced option
- Schedule: Advanced - Show advanced option
- Gateway:** GW_OPT1 - 10.0.127.10 (highlighted)
- In/Out: Advanced - Show advanced option
- Ackqueue/Queue: Advanced - Show advanced option
- Layer7: Advanced - Show advanced option

Вместо IP провайдера в поле Gateway IP адрес от провайдера динамический (DHCP),

Автор:

15.10.12 13:32 - Последнее обновление 15.10.12 20:44

System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Help

General configuration

Enable **Enable Interface**

Description
Enter a description (name) for the interface here.

Type

MAC address
Insert my local MAC address
This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.

MSS
If you enter a value in this field, the MSS value entered above minus 40 (TCP/IP header size) will be in effect.

PPTP/L2TP configuration

Username

Password

Local IP address /

Remote IP address

Dial on demand **Enable Dial-On-Demand mode**
This option causes the interface to operate in dial-on-demand mode, allowing you to have a *virtual full time* connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

Idle timeout seconds
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

Advanced [Click here for additional PPTP and L2TP configuration options. Save first if you made changes.](#)

Private networks

Block private networks
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on unless your network is a private network.

www.thin.kiev.ua/2012/10/15/pfsense-2.0-pptp-client-on-wan/