

Автор:

10.09.12 12:18 - Последнее обновление 14.03.13 14:57

PPTP сервер на WAN + Squid + SquidGuard и доступ в интернет в PfSense 2.0

Настройка PPTP сервера и фильтра доступа Squid + SquidGuard были в статьях опубликованных ранее.

<http://thin.kiev.ua/router-os/50-pfsense/402--pptp-server-pfsense-20.html>

<http://thin.kiev.ua/router-os/50-pfsense/530-pfsense-squid.html>

<http://thin.kiev.ua/router-os/50-pfsense/549-hav.htm>

<http://thin.kiev.ua/router-os/50-pfsense/533--pfsense-transparent-squid-ip-.html>

Если вы подняли PPTP сервер на WAN интерфейсе вместе с фильтром Squid + SquidGuard, подключились к PPTP серверу и увидели сообщение:

**ОШИБКА
Запрошенный URL не может быть доставлен**

Во время доставки UR<http://www.google.com>

Автор:

10.09.12 12:18 - Последнее обновление 14.03.13 14:57

Произошла следующая ошибка:

- **Доступ запрещён.**

Настройка контроля доступа не даёт возможности выполнить Ваш запрос в настоящее время.
Пожалуйста, свяжитесь с Вашим поставщиком услуг Интернет, если Вы считаете это неправильным.

Generated Mon, 10 Sep 2012 10:17:10 GMT by steel.lan (squid/2.7.STABLE9)

ОШИБКА

Запрошенный URL не может быть доставлен

Во время доставки URL: <http://www.google.com/>

Произошла следующая ошибка:

- Доступ запрещён.

Настройка контроля доступа не даёт возможности выполнить Ваш запрос в настоящее время. Пожалуйста, свяжитесь с Вашим поставщиком услуг Интернет, если Вы считаете это неправильным.

Generated Mon, 10 Sep 2012 10:17:10 GMT by steel.lan (squid/2.7.STABLE9)

Есть три варианта решения:

1. В настройках PPTP клиента убрать галочку

Автор:

10.09.12 12:18 - Последнее обновление 14.03.13 14:57

The screenshot shows the PfSense web interface with two main windows open:

- Top Window: Дополнительные параметры TCP/IP (Additional TCP/IP parameters)**
 - General Tab:** Describes how IP parameters can be assigned during simultaneous connection to the local network and the remote access network. It includes options for automatic IP assignment and using a static IP.
 - DNS Tab:** Contains the checked checkbox **Использовать основной шлюз в удаленной сети** (Use primary gateway in remote network), which is highlighted with a red box.
 - Wins Tab:** Not visible in the screenshot.
- Bottom Window: VPN: VPN PPTP (Configuration tab)**
 - PPTP redirection:** Options for turning off PPTP or redirecting incoming connections to a specific IP address. The "off" option is selected.
 - No. PPTP users:** Set to 10.
 - Server address:** Set to 192.168.0.50.
 - Remote address range:** Set to 192.168.0.51.
 - PPTP DNS Servers:** Primary server set to 192.168.0.1, secondary to 8.8.8.8.
 - WINS Server:** Not specified.

Both windows have a blue border, and the entire screenshot is framed by a thick blue border. A red box highlights the "Use primary gateway in remote network" checkbox in the TCP/IP settings window. Another red box highlights the "Server address" field in the PPTP configuration window. A third red box highlights the "Primary DNS server" field in the PPTP DNS Servers list.

Автор:

10.09.12 12:18 - Последнее обновление 14.03.13 14:57

VPN: VPN PPTP

Configuration Users

PPTP redirection

No. PPTP users: 10

Server address: 192.168.20.1

Remote address range: 192.168.20.2

PPTP DNS Servers: 192.168.20.1, 8.8.8.8

Interfaces: OPT1

General configuration

Description: OPT1

Type: Static

IP address: 192.168.20.1

Gateway: None

Private networks

Block private networks:

Block loopback networks:

Далее настраиваем SQUID

4 / 7

Автор:

10.09.12 12:18 - Последнее обновление 14.03.13 14:57

Interfaces: OPT1

General configuration

Enable **Enable Interface**

Description: OPT1
Enter a description

Type: Static

MAC address: This field can be set by the ISP (may be required). Enter a MAC address.

MTU: If you leave this blank, the system'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.

Proxy server: Insert my local MAC address ("") the MAC address of this interface

RIP:

SNMP:

UPnP & NAT-PMP: Wake on LAN:

Proxy server: General settings

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Proxy interface WAN LAN OPT1 loopback The interface(s) the proxy will listen to.

Allow users on interface If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.

Transparent proxy If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.

Bypass proxy for Private Address Space (RFC 1918) destination: Do not forward traffic to Private Address Space (RFC 1918) **destination** through the proxy server but directly through the firewall.

Bypass proxy for these source IPs: Do not forward traffic from these **source** IPs, CIDR nets, hostnames, or aliases through the proxy server but directly through the firewall. Separate by semi-colons (;). [Applies only to transparent mode]

Bypass proxy for these destination IPs: Do not proxy traffic going to these **destination** IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. Separate by semi-colons (;). [Applies only to transparent mode]

Proxy server: General settings

General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Proxy interface WAN LAN OPT1 loopback The interface(s) the proxy will listen to.

Allow users on interface If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.

Transparent proxy If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.

Bypass proxy for Private Address Space (RFC 1918) destination: Do not forward traffic to Private Address Space (RFC 1918) **destination** through the proxy server but directly through the firewall.

Bypass proxy for these source IPs: Do not forward traffic from these **source** IPs, CIDR nets, hostnames, or aliases through the proxy server but directly through the firewall. Separate by semi-colons (;). [Applies only to transparent mode]

Автор:

10.09.12 12:18 - Последнее обновление 14.03.13 14:57

Proxy filter SquidGuard: Groups Access Control List (ACL)

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log

Disabled	Name	Time	Description	Actions
on	BAD		BAD	
on	VIP		VIP	
	PPTP	WorkTime		
	WorkTimeGROUP	WorkTime	WorkTimeGROUP	

Найти: rrrr Следующее ↑ Предыдущее ↺ Подсветить все Учесть регистр

пуск

pfSense.lan - Proxy f... squid-a28.jpg - Paint Моя рабочий

System Interfaces Firewall Services VPN Status Diagnostics Help

RU 10:35 вторник 11.09.2012

Proxy filter SquidGuard: Groups Access Control List (ACL)

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log

Disabled	Name	Time	Description	Actions
on	BAD		BAD	
on	VIP		VIP	
	PPTP	WorkTime		
	WorkTimeGROUP	WorkTime	WorkTimeGROUP	

Автор:

10.09.12 12:18 - Последнее обновление 14.03.13 14:57

Proxy filter SquidGuard: Groups Access Control List (ACL): Edit

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log

Disabled Check this for disable this ACL rule.

Name **PPTP**

Order **.....** Select the new position for ACL item. ACL are evaluated on a first-match source basis.
Note: Search for a suitable ACL by field 'source' will occur before the first match. If you want to define an exception for some sources (IP) from the IP range, put them on first of the list.
For example: ACL with single (or short range) source ip 10.0.0.15, must be placed before ACL with more large ip range 10.0.0.0/24

Client (source) **192.168.20.0/24**

Time Work Time Select time in which 'Target Rules' will operate, or leave 'none' for action of rules without time restriction. If this option is set, then in off-time will operate the second rule set.

Target Rules **!FileAccessDeny ^~Wite-List !blk_BL_porn all [!FileAccessDeny ^~Wite-List !blk_BL_porn all]**

Not to allow IP addresses in URL To make sure that people don't bypass the URL filter, by simply using the IP addresses instead of the fully qualified domain names, you can check this option. This option has no effect on the WhiteList.

Proxy filter SquidGuard: General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log

Enable Check this for enable squidGuard
For saving configuration YOU need click button 'Save' on bottom of page
After changing configuration squidGuard you must **apply all changes**

Apply **STARTED**

Enable GUI log Check this for enable GUI log.

Enable log Check this for enable log of the proxy filter. Usually log used for testing filter settings.

Enable log rotation Check this for enable daily rotate a log of the proxy filter. Use this option for limit log file size.

Clean Advertising Check this to display a blank gif image instead the default block page. With this option you get a cleaner page.

Blacklist options

Blacklist

http://thin.kiev.ua/router/2os/501676177721013513265855/pfSense-20.html