

Jamsux's Blog

abril 4, 2010

Pfsense + Squid (transparent)

Filed under: Uncategorized — jamsux @ 5:06 am

Bom, ultimamente tive a necessidade de implementar um proxy em um cliente, só que pelo fato da estrutura dele ser pequena não precisava instalar mais uma VM, mais um serviço, ter dois sistemas e tal.

Foi quanto decidi implementar no Pfsense mesmo, instalei o pacote e experimentei, Finalizando foi um sucesso, sanei duas dificuldade com apenas uma solução, show de bola, então vou postar logo abaixo um tutozinho de como fazer essa implementação, do Pfsense com proxy transparent.

Primeiro precisamos instalar o pacote do Squid, para isso vamos em **Packages**, procure o pacote **Squid** e clique no sinal + (mais).

		platform: 1.0	forum	information about system facts like Uptime, CPU, Memory, PCI devices, SCSI devices, IDE devices, Network adapters, Disk usage, and more.	
rate	Network Management	BETA 0.9 platform: 1.2.2	No info, check the forum	This package adds a table of realtime bandwidth usage by IP address to Status -> Traffic Graphs	
snort	Security	Stable 2.8.5.3 pkg v. 1.19 platform: 1.2.3	Package Info	Used by fortune 500 companies and governments Snort is the most widely deployed IDS/IPS technology worldwide. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more.	
snort-old	Security	legacy 2.8.4.1_5 pkg v.1.7 platform: 1.2.2	Package Info	WARNING: This is the old snort package. A few current snort.org rules are not supported in this package. This package will not be supported in Pfsense 2.0.	
squid	Network	Stable 2.7.8.1 platform: 1.2.1	No info, check the forum	High performance web proxy cache.	
squid3	Network	ALPHA 3.0.8_09 platform: 1.2.1	No info, check the forum	EXPERIMENTAL! Not all directives are ported yet! High performance web proxy cache.	
squidGuard	Network Management	Beta 1.3-2 platform: 1.1	No info, check the forum	High performance web proxy URL filter. Required proxy Squid package.	
stunnel	Network Management	Stable 4.30.2 platform:	Package Info	An SSL encryption wrapper between remote client and local or remote servers.	

Após fazer a instalação do pacote aparecerá na opção **Services / Proxy Server**

System

- Advanced
- Firmware
- General Setup
- Packages
- Setup wizard
- Static routes

Interfaces

- (assign)
- WAN
- LAN

Firewall

- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

Services

- Captive portal
- DNS forwarder
- DHCP relay
- DHCP server
- Dynamic DNS
- Load Balancer
- OLSR
- PPPoE Server
- RIP
- SNMP
- UPnP
- OpenNTPD
- Wake on LAN
- siproxd
- Proxy server**

VPN

- IPsec
- OpenVPN
- PPTP

Proxy server: General settings

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

Proxy interface	LAN WAN The interface(s) the proxy server will bind 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 through the proxy server but directly through the firewall. Separate by semi-colons (;).
Enabled logging	☐ This will enable the access log. Don't switch this on if you don't have much disk space left.
Log store directory	/var/squid/log The directory where the log will be stored (note: do not end with a / mark)
Log rotate	Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
Proxy port	3128 This is the port the proxy server will listen on.

Depois, configure as opções **Proxy interface**, **Allow Users**, **Transparent proxy**, **enabled Logging** e **Proxy** como na figura a seguir:

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

Proxy interface	LAN WAN The interface(s) the proxy server will bind to.	Interface onde o proxy trabalhará LAN
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.	Permitir usuários na interface
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.	Habilitar todo o tráfego da porta 80, Proxy transparent
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 through the proxy server but directly through the firewall. Separate by semi-colons (;).	
Enabled logging	☒ This will enable the access log. Don't switch this on if you don't have much disk space left.	Habilite o Log para poder fazer a autoria posteriormente
Log store directory	/var/squid/log The directory where the log will be stored (note: do not end with a / mark)	Diretório do Log
Log rotate	Defines how many days of logfiles will be kept. Rotation is disabled if left empty.	
Proxy port	3128 This is the port the proxy server will listen on.	Porta padrão do proxy - 3128
ICP port	This is the port the Proxy Server will send and receive ICP queries to and from neighbor caches. Leave this	

CLIQUE EM SAVE

Depois clique na opção **Cache Mgmt**



webConfigurator

jamsux-pfsense.local

System

Advanced

Firmware

General Setup

Package

Setup wizard

Static routes

Interfaces

(assign)

WAN

LAN

Firewall

Aliases

NAT

Rules

Schedules

Traffic Shaper

Virtual IPs

Services

Captive portal

DNS forwarder

DHCP relay

DHCP server

Dynamic DNS

Load Balancer

OLSR

PPPoE Server

RIP

SNMP

UPnP

OpenNTPD

Wake on LAN

Proxy server: Cache management

General

Upstream Proxy

Cache Mgmt

Access Control

Traffic Mgmt

Auth Settings

Local Users

Hard disk cache size

100

Tamanho do cache do disco -> aconselhavel deixar mais q 1 GB

This is the amount of disk space (in megabytes) to use for cached objects.

Hard disk cache system

aufs

This specifies the kind of storage system to use.

ufs is the old well-known Squid storage format that has always been there.

aufs uses POSIX-threads to avoid blocking the main Squid process on disk-I/O. (Formerly known as async-io.)

diskd uses a separate process to avoid blocking the main Squid process on disk-I/O.

Hard disk cache location

/var/squid/cache

Localização do Cache

This is the directory where the cache will be stored. (note: do not end with a /). If you change this location, squid needs to make a new cache, this could take a while

Memory cache size

8

Qtde Memória Ram para Cache

This is the amount of physical RAM (in megabytes) to be used for negative cache and in-transit objects. This value should not exceed more than 50% of the installed RAM. The minimum value is 1MB.

Minimum object size

0

Objects smaller than the size specified (in kilobytes) will not be saved on disk. The default value is 0, meaning there is no minimum.

Maximum object size

4

Objects larger than the size specified (in kilobytes) will not be saved on disk. If you wish to increase speed

Management

Queues

RRD Graphs

Services

System

System logs

Traffic graph

UPnP

Diagnostics

ARP Tables

Backup/Restore

Command Prompt

Edit File

Factory defaults

Halt system

Ping

Reboot system

Routes

Sniff

Traceroute

Packet Capture

ntop Settings

ntop

(possibly popular) objects.

Heap LFUDA: Least Frequently Used with Dynamic Aging

The Heap LFUDA policy keeps popular objects in cache regardless of their size and thus optimizes byte hit rate at the expense of hit rate since one large, popular object will prevent many smaller, slightly less popular objects from being cached.

Heap LRU: Last Recently Used

Works like LRU, but uses a heap instead.

Note: If using the LFUDA replacement policy, the value of Maximum Object Size should be increased above its default of 12KB to maximize the potential byte hit rate improvement of LFUDA.

Cache replacement policy

Heap LFUDA

The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. The default policy for cache replacement is LFUDA. Please see the type descriptions specified in the memory replacement policy for additional detail.

Low-water-mark in %

90

Cache replacement begins when the swap usage is above the low-low-water mark and attempts to maintain utilisation near the low-water-mark.

High-water-mark in %

95

As swap utilisation gets close to the high-water-mark object eviction becomes more aggressive.

Do not cache

Enter each domain or IP address on a new line that should never be cached.

Você pode listar aqui, os dominios que não serão armazenados em cache

Enable offline mode

Enable this option and the proxy server will never try to validate cached objects. The offline mode gives access to more cached information than the proposed feature would allow (stale cached versions, where the origin server should have been contacted).

Save

Depois é só configurar os sites que você vai bloquear e permitir, para isso você clica em **Access Control**



webConfigurator

jamsux-pfsense.local

System

Advanced

Firmware

General Setup

Package

Setup wizard

Static routes

Interfaces

(assign)

WAN

LAN

Firewall

Aliases

NAT

Rules

Schedules

Traffic Shaper

Virtual IPs

Services

Captive portal

DNS forwarder

DHCP relay

DHCP server

Dynamic DNS

Load Balancer

OLSR

PPPoE Server

RIP

SNMP

UPnP

OpenNTPD

Wake on LAN

Proxy server: Access control

General

Upstream Proxy

Cache Mgmt

Access Control

Traffic Mgmt

Auth Settings

Local Users

Allowed subnets

10.0.0.0/24

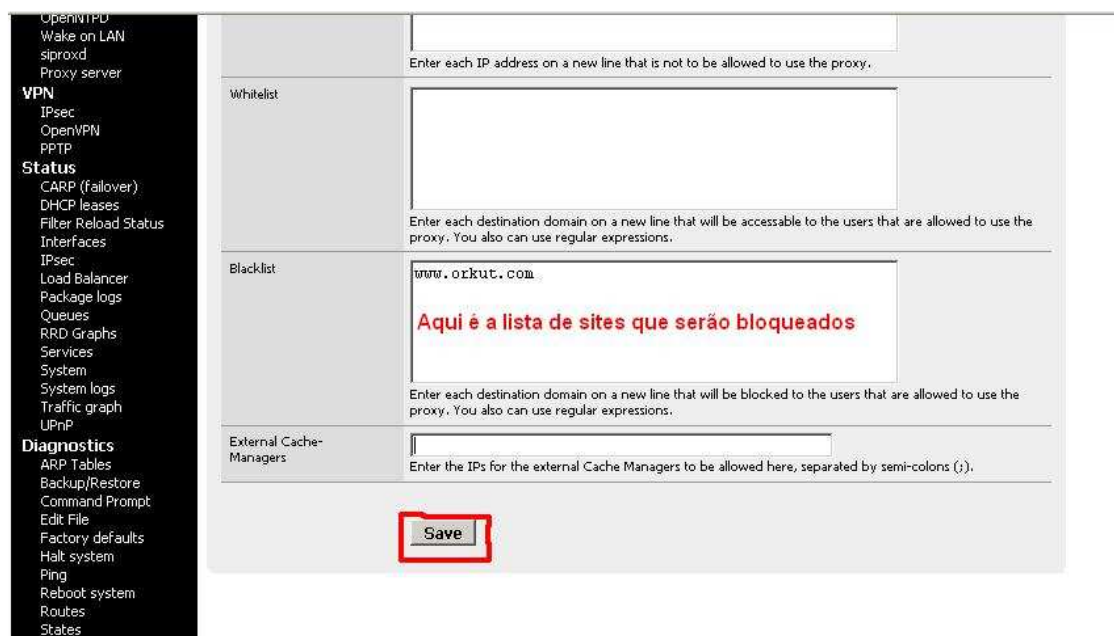
Digite aqui a rede que o proxy estará ativado, no meu caso minha rede interna

Enter each subnet on a new line that is allowed to use the proxy. The subnets must be expressed as CIDR ranges (e.g.: 192.168.1.0/24). Note that the proxy interface subnet is already an allowed subnet. All the other subnets won't be able to use the proxy.

Unrestricted IPs

Enter each unrestricted IP address on a new line that is not to be filtered out by the other access control directives set in this page.

Banned host addresses



Pronto! Seu proxy transparent está no ar, agora é só testar!

Comentários (4)

4 Comentários »

1. Muito bom kra, ajudou muito obrigado!!

Comentário por josue — maio 11, 2011 @ 12:43 am

Responder

2. Muito bom tutorial.. parabéns.. Porém ainda estou com um problema e não sei como solucionar. Fiz todo o procedimento que vc postou só que não funciona em modo transparente. Só funciona se eu coloco proxy no navegador. Se eu tiro o proxy do navegador a navegação não passa pelas regras (fica tudo aberto)

Comentário por Fábio — maio 15, 2011 @ 4:56 pm

Responder

- Olá Fábio,

Qual a versão do seu PfSense? Essa configuração não tem erro. Olha só, me envia o XML pra eu dar uma olhada (pode retirar as informações que vc achar pertinente)

Pode enviar pra meu e-mail: jamsux at gmail dot com

Qualquer situações entre em contato por e-mail que te ajudo.

Comentário por jamsux — maio 18, 2011 @ 1:22 pm

Responder

3. vlw, cara muito bom msm.
continue com os tutor..

Comentário por Thiago — agosto 29, 2011 @ 5:36 pm

Responder

Feed RSS (Really Simple Syndication) para comentários sobre este post. [URI \(Uniform Resource Identifier\) de trackback](#)

Tema: Silver is the New Black. [Blog no WordPress.com](#).

Seguir

Follow “Jamsux's Blog”

Powered by [WordPress.com](#)