

Sumário

| | |
|--|----|
| Geração da mídia de instalação..... | 1 |
| Instalação do Sistema Operacional:..... | 2 |
| Configuração inicial da LAN via console..... | 6 |
| Assistente de configuração inicial..... | 8 |
| Certificado https..... | 14 |
| Instalação dos pacotes nativos..... | 14 |
| Squid..... | 16 |
| Ajustes Squid..... | 18 |
| Instalação dos pacotes Pré-Compilados..... | 29 |
| Dansguardian..... | 30 |
| Sarg..... | 33 |
| DHCP Server..... | 36 |
| Configuração automática do Proxy..... | 37 |
| Bloqueio de acessos por fora do Proxy..... | 38 |
| Finalizando..... | 41 |

Geração da mídia de instalação

Iniciar o servidor a partir da mídia de instalação desejada, CD, DVD ou Pendrive.

As mídias de instalação estão disponíveis através do site do projeto PFSense, mais especificamente na URL abaixo:

<https://www.pfsense.org/download/>

Caso opte por CD ou DVD, pode ser utilizado qualquer aplicativo comum de gravação de CDs ou DVDs como por exemplo, Nero, Brasero, K3B, etc.

Ou se a opção for utilizar um pen drive, segue o procedimento indicado pelo próprio projeto PFSense para a gravação (a partir de uma estação like unix):

Writing Images in UNIX

On UNIX and UNIX-like systems, dd is the best choice for writing disks.

Linux/other

The dd command on Linux may be used from a shell logged in as a user with **sudo** access or the root user [Collapse] directly.

Before proceeding, check the system log or run the dmesg command after connecting the target disk to find its device name (e.g. /dev/sdd or something like /dev/mmcblk0 if systemd is in use). The following commands use sample disk names, replace them with the actual device name of the target disk.

The image can be decompressed and written in one command. If run as root, omit **sudo**.

```
$ gzip -dc pfSense-memstick-2.2.3-RELEASE-amd64.img.gz | sudo dd of=/dev/sdz bs=1M
[sudo] password for user:
0+7416 records in
0+7416 records out
243048448 bytes (243 MB) copied, 26.3313 s, 9.2 MB/s
$
```

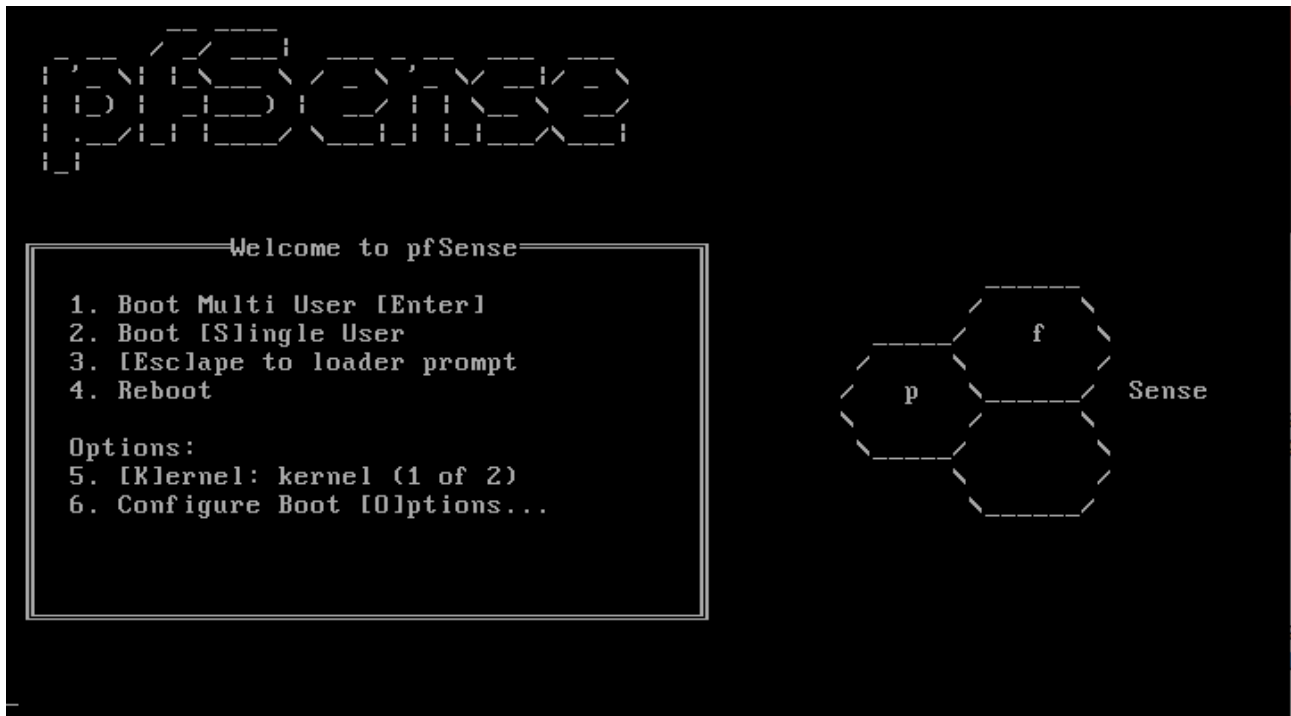
If a warning is printed about "trailing garbage" it may be safely ignored, as it is from the file's digital signature.

Obs.: Maiores informações para a gravação da mídia a partir de outros sistemas operacionais podem ser obtidas através da URL abaixo:

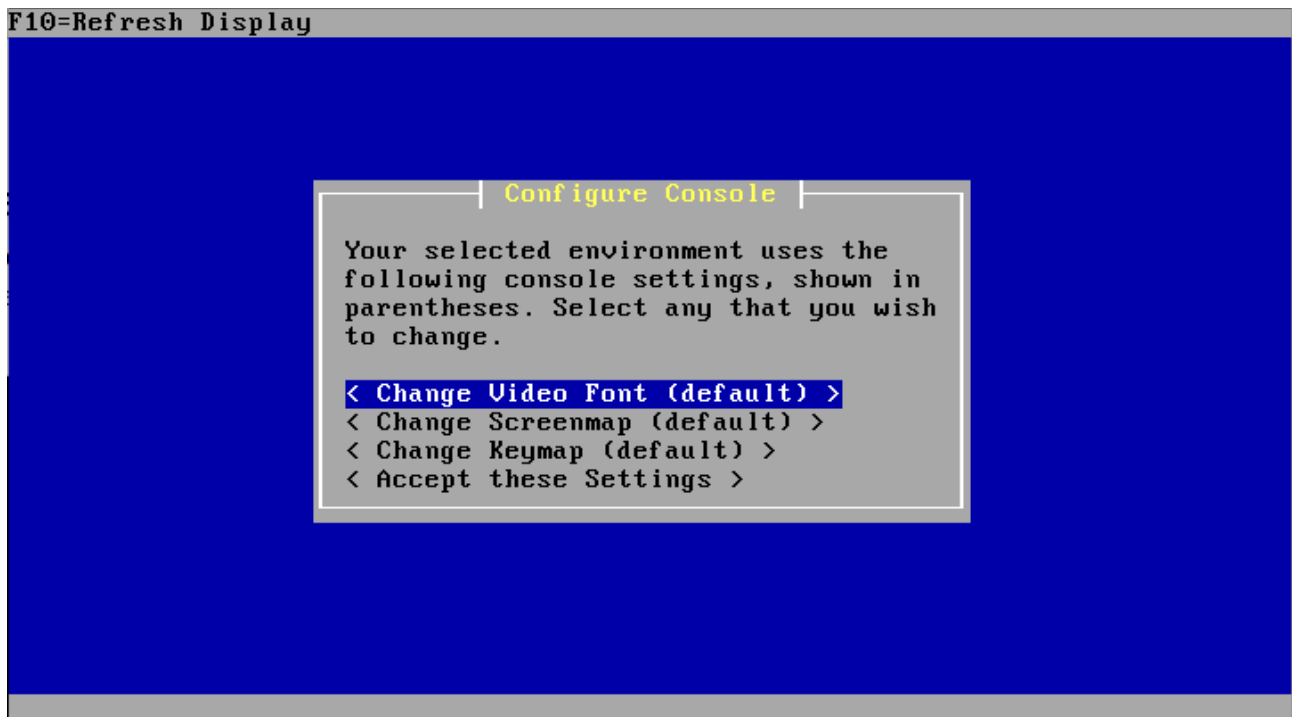
https://doc.pfsense.org/index.php/Writing_Disk_Images

Instalação do Sistema Operacional:

Conecte o pen drive à porta USB ou insira a mídia no leitor, configure a BIOS do servidor para iniciar a partir da opção desejada e aguarde até que seja carregada a tela inicial da instalação conforme a imagem a seguir:



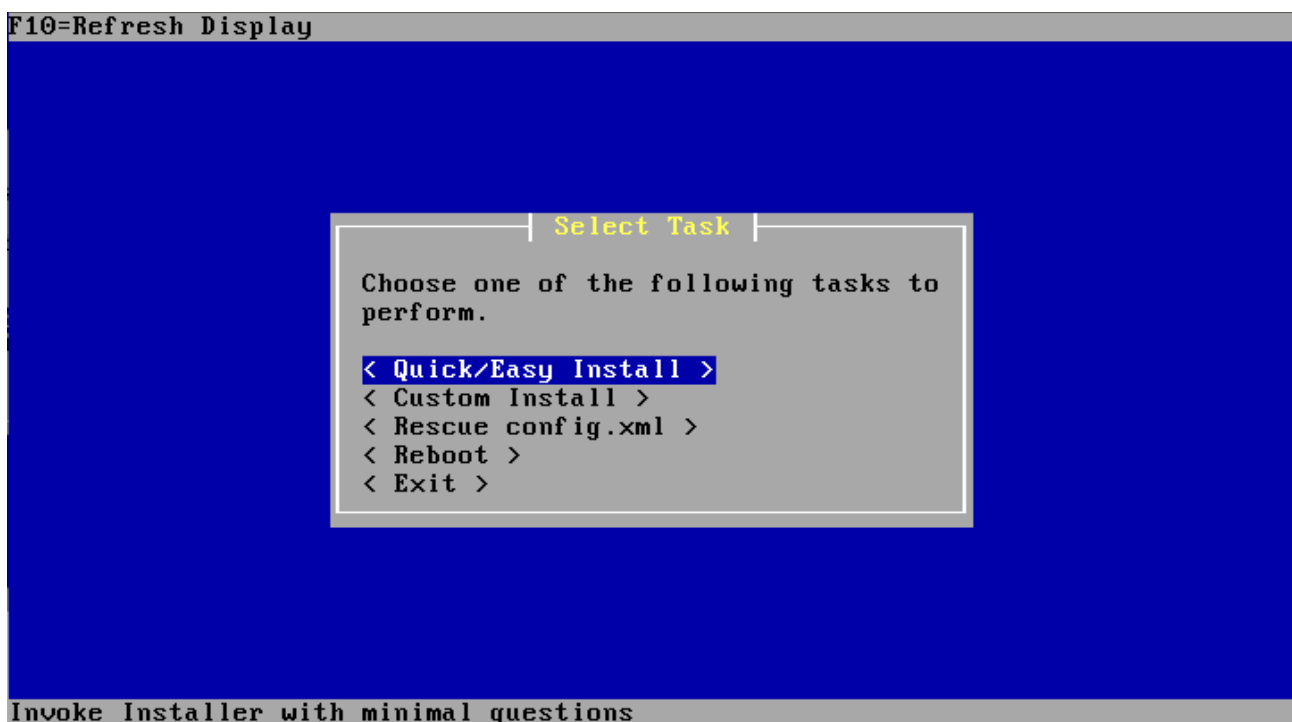
Escolha a opção padrão 1 e confirme com <enter> ou apenas aguarde alguns segundos para que a instalação prossiga automaticamente para a próxima tela conforme a imagem a seguir:



Normalmente não é necessário efetuar nenhum ajuste porém se for preciso, utilize essas opções para adequar as configurações de vídeo e mapeamento de teclado.

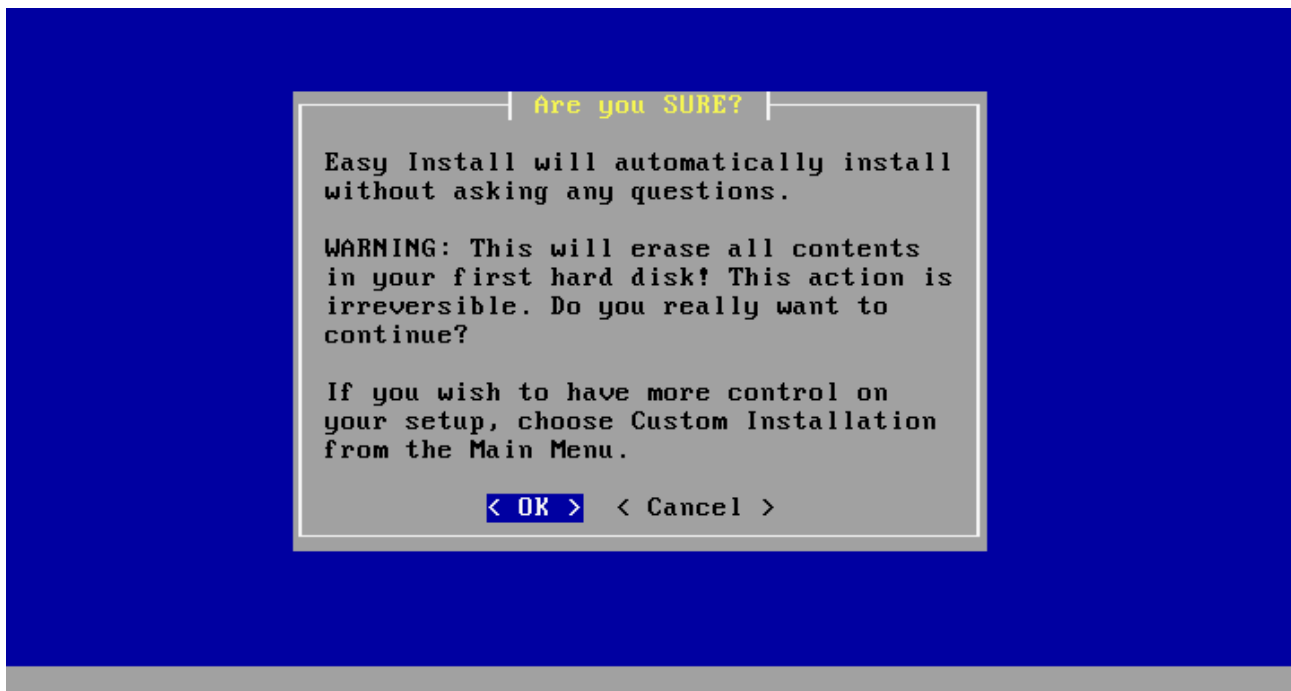
Quando finalizado prossiga com a última opção (Accept these Settings).

Em seguida será o menu de tipo de instalação.

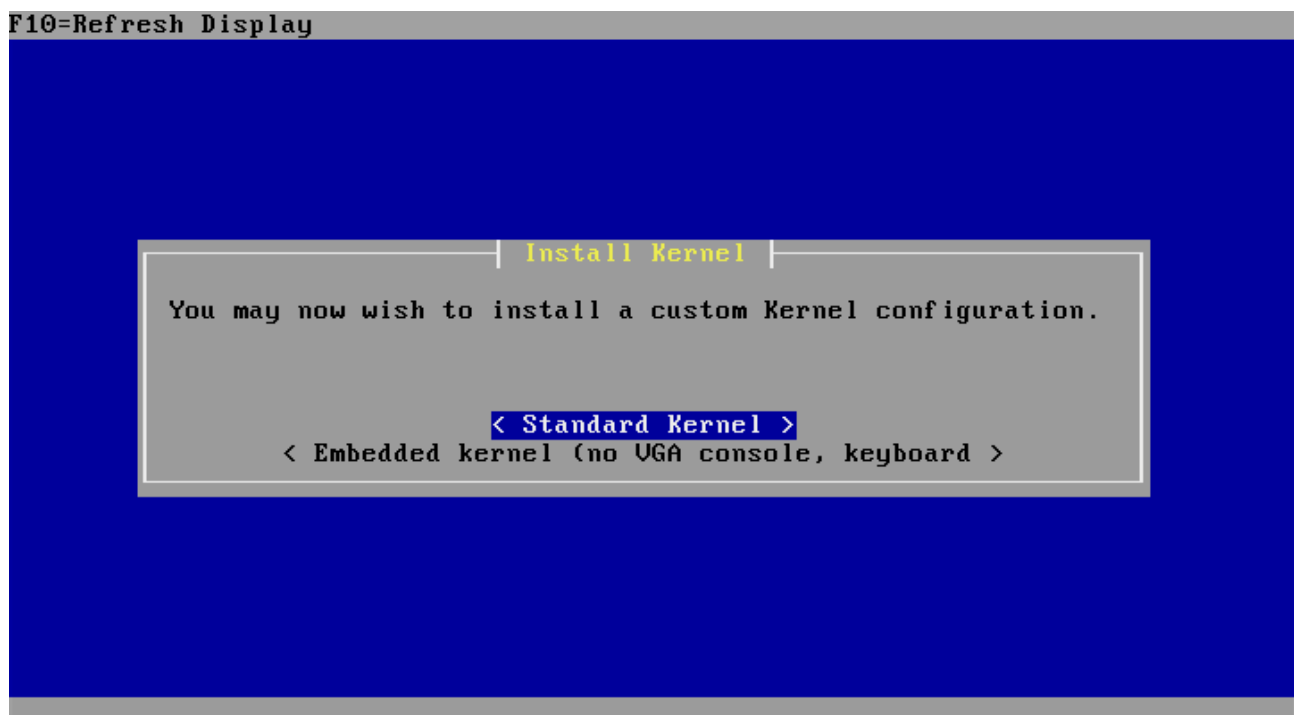


Para esse projeto podemos utilizar a instalação padrão (Quick/Easy Install).

A tela a seguir é apenas uma advertência avisando que não serão feitas mais perguntas e que o conteúdo do primeiro disco rígido será perdido.

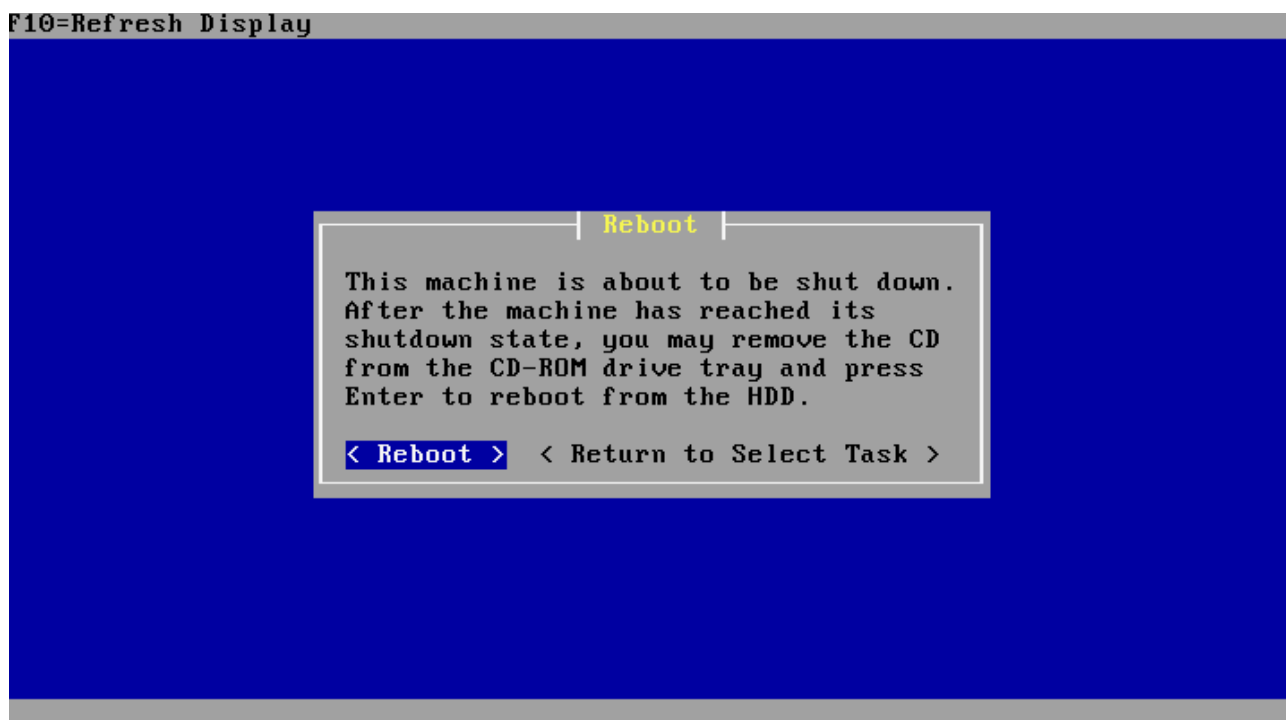


Basta confirmar com OK e será a última etapa da instalação que é a escolha do kernel.



Para esse projeto, utilizaremos o kernel padrão (Standard Kernel).

A partir disso nossa instalação está concluída.



Remova a mídia de instalação e confirme com a opção Reboot para iniciar o servidor a partir do Sistema instalado.

Configuração inicial da LAN via console

A imagem abaixo exibe o menu inicial de console do Sistema.

A primeira interface de rede, sugestivamente, assume o papel da interface WAN (onde deve ser conectada o link de internet) e as demais são para DMZs internas, como por exemplo a LAN.

Por padrão de instalação, o PFSense vem com a interface LAN configurada com o IP estático 192.168.1.1 conforme podemos ver na imagem a seguir.

```
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3.1-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Caso queiramos alterar esse IP da rede LAN, podemos fazê-lo através da opção de menu número 2, Set interface(s) IP address e em seguida novamente a opção 2, LAN.

```
*** Welcome to pfSense 2.3.1-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
```

Será solicitado para que informemos o IP desejado, que nessa ocasião utilizaremos o IP 10.10.2.12/24.

Preencha primeiramente o IP e na próxima solicitação a subnet conforme a imagem a seguir:

```
Enter an option: 2

Available interfaces:

1 - WAN (em0)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.2.12

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Em segui será solicitado um endereço de gateway (caso estivéssemos configurando a interface WAN) que nessa ocasião deixaremos em branco, Ipv6 que também não iremos utilizar e por fim se desejamos ativar um servidor DHCP na interface (escolhi não pois faremos via a interface web posteriormente).

A partir desse momento, terminamos as configurações iniciais via console e já podemos utilizar a interface de gerenciamento WEB pela URL informada conforme a imagem a seguir (10.10.2.12 nesse caso).

```
For a WAN, enter the new LAN IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
>  
  
Enter the new LAN IPv6 address. Press <ENTER> for none:  
>  
  
Do you want to enable the DHCP server on LAN? (y/n) n  
Disabling IPv4 DHCPD...Disabling IPv6 DHCPD...  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n  
  
Please wait while the changes are saved to LAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...  
  
The IPv4 LAN address has been set to 10.10.2.12/24  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
        https://10.10.2.12/  
  
Press <ENTER> to continue.
```


Assistente de configuração inicial

Como dito anteriormente, a partir desse momento toda a configuração será feita através da interface WEB.

Por padrão o usuário administrador é “admin” e a senha é “pfsense”.

A screenshot of the pfSense login interface. It has a dark grey header with the text 'Login to pfSense' in white. Below the header is a white box containing the login form. The form has two fields: 'Username' with the value 'admin' and 'Password' with masked characters '.....'. A blue 'Login' button is positioned below the password field.

Após o primeiro login, iremos acessar o assistente de configuração inicial conforme a imagem a seguir, apenas clique em Next.

A screenshot of the pfSense Setup Wizard. The top navigation bar includes the pfSense logo and various menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. Below the navigation bar is a breadcrumb trail: 'Wizard / pfSense Setup /'. The main content area is titled 'pfSense Setup' and contains two lines of text: 'This wizard will provide guidance through the initial configuration of pfSense.' and 'The wizard may be stopped at any time by clicking the logo image at the top of the screen.' At the bottom of the content area is a blue button with a right arrow and the text 'Next'.

O PFSense possui uma versão paga, chamada Gold, porém não entraremos nessa questão e utilizaremos a versão gratuita. Apenas clique Next novamente:

Sen e
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Gold ▾ Help ▾

Wizard / pfSense Setup / Bling your pfSense with pfSense Gold

Bling your pfSense with pfSense Gold

Feel the power of a pfSense Gold subscription. Receive special benefits while supporting ongoing development of the Open Source pfSense project.

Benefits include access to our AutoConfigBackup secure cloud based backup service for up to 10 hosts, pre-publication access to the updated pfSense: The Definitive Guide book in PDF, fully updated for the pfSense 2.1 release, and a monthly online MeetUp! Video conference to discuss and demonstrate advanced features and architectures using pfSense.

Go to [pfSense Gold Subscriptions](#) to sign up now.

» Next

A próxima etapa é a configuração de hostname e servidores DNS:

Sen e
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Gold ▾ Help ▾

Wizard / pfSense Setup / General Information

General Information

On this screen the general pfSense parameters will be set.

Hostname
EXAMPLE: myserver

Domain
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS ☒ Allow DNS servers to be overridden by DHCP/PPP on WAN

» Next

Em seguida o TimeZone e o servidor de horas:

Sen e
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Gold ▾ Help ▾

Wizard / pfSense Setup / Time Server Information

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

» Next

E por final temos a configuração da Interface WAN que pode ser configurada de diversas formas:

1. Estticamente (como será o caso agora):

Selecionamos no box inicial (Selected Type) a opção Static e preenchemos as informações na seção Static IP Configuration.

The screenshot shows the 'Configure WAN Interface' window. At the top, it says 'On this screen the Wide Area Network information will be configured.' Below this, the 'SelectedType' dropdown is set to 'Static'. The 'General configuration' section contains three fields: 'MAC Address' (empty), 'MTU' (empty), and 'MSS' (empty). Each field has a descriptive text below it. The 'Static IP Configuration' section at the bottom contains three fields: 'IP Address' (10.10.1.77), 'Subnet Mask' (32), and 'Upstream Gateway' (10.10.1.94).

| Configure WAN Interface | |
|--|---|
| On this screen the Wide Area Network information will be configured. | |
| SelectedType | Static |
| General configuration | |
| MAC Address | <input type="text"/> <small>This field can be used to modify ("spoof") the MAC address of the WAN 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.</small> |
| MTU | <input type="text"/> <small>Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.</small> |
| MSS | <input type="text"/> <small>If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.</small> |
| Static IP Configuration | |
| IP Address | <input type="text" value="10.10.1.77"/> |
| Subnet Mask | <input type="text" value="32"/> |
| Upstream Gateway | <input type="text" value="10.10.1.94"/> |

Obs.: Essa interface é a interface WAN, ou seja, a interface pública. Provavelmente teremos aqui um IP válido de internet e um gateway também com endereço de internet válido. Estamos utilizando o endereço 10.10.1.94 por estarmos apenas fazendo uma demonstração dentro de uma subrede interna.

2. DHCP:

DHCP é uma opção muito comum para cliente que possuem links empresariais ou links dedicados.

Basta selecionar a opção DHCP no box inicial (Selected Type).

The screenshot shows the 'Configure WAN Interface' window. At the top, it says 'On this screen the Wide Area Network information will be configured.' Below this, the 'SelectedType' dropdown is set to 'DHCP'.

| Configure WAN Interface | |
|--|------|
| On this screen the Wide Area Network information will be configured. | |
| SelectedType | DHCP |

3. PPPoE:

PPPoE é a opção mais comum para clientes com links domésticos como por exemplo Speedy.

Selecione a opção PPPoE no box inicial (Selected Type).

| Configure WAN Interface | |
|--|-------|
| On this screen the Wide Area Network information will be configured. | |
| SelectedType | PPPoE |

E preencha os dados na seção PPPoE Configuration:

| PPPoE configuration | |
|----------------------|---|
| PPPoE Username | username@provedor.com.br |
| PPPoE Password | |
| Show PPPoE password | <input type="checkbox"/> Reveal password characters |
| PPPoE Service name | Speedy <small>Hint: this field can usually be left empty</small> |
| PPPoE Dial on demand | <input type="checkbox"/> Enable Dial-On-Demand mode <small>This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.</small> |
| PPPoE Idle timeout | <input type="text"/> <small>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.</small> |

4. PPTP:

Conexões do tipo PPTP são raramente utilizadas porém se necessário pode ser configurada assim como os outros métodos.

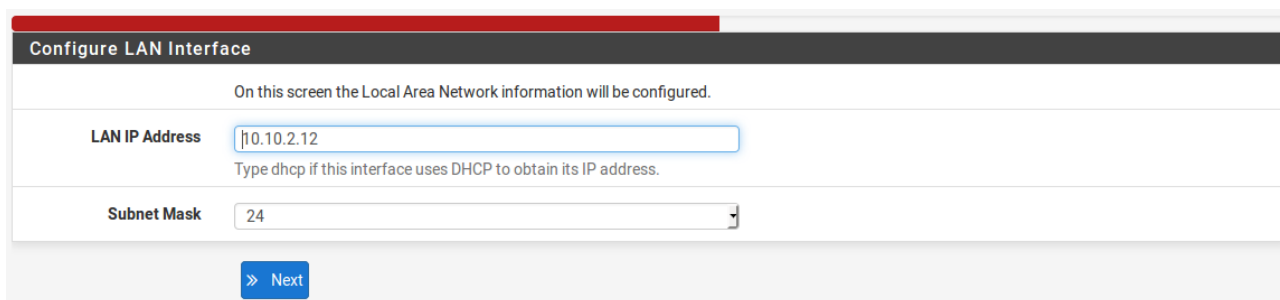
Selecione PPTP no box inicial (Selected Type).

| Configure WAN Interface | |
|--|------|
| On this screen the Wide Area Network information will be configured. | |
| SelectedType | PPTP |

E informe os dados de conexão na sessão PPTP configuration

| PPTP configuration | |
|------------------------|---|
| PPTP Username | username |
| PPTP Password | |
| Show PPTP password | <input type="checkbox"/> Reveal password characters |
| PPTP Local IP Address | 10.10.2.254 |
| pptplocalsubnet | 32 |
| PPTP Remote IP Address | x.x.x.x |
| PPTP Dial on demand | <input type="checkbox"/> Enable Dial-On-Demand mode <small>This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.</small> |
| PPTP Idle timeout | <input type="text"/> <small>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.</small> |

Em seguida temos a opção de alterar as configurações feitas previamente através do console, quando setamos a interface LAN porém como já configuramos com o IP desejado basta proceder clicando em Next.



Configure LAN Interface

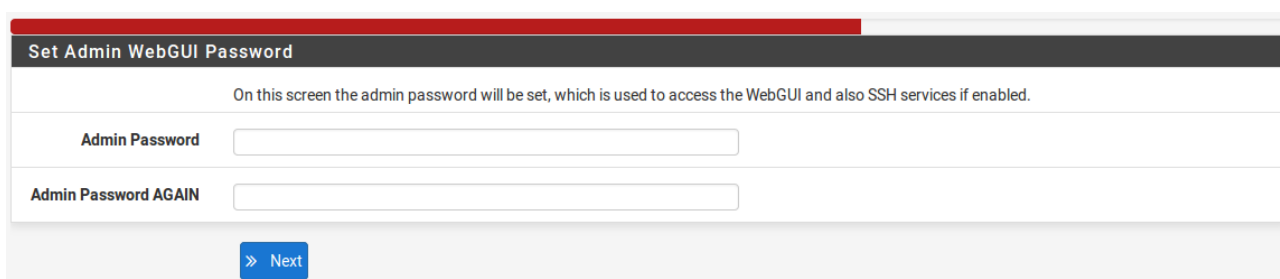
On this screen the Local Area Network information will be configured.

LAN IP Address
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

[Next](#)

Por final podemos (e devemos por questões de segurança) alterar a senha padrão do usuário admin.



Set Admin WebGUI Password

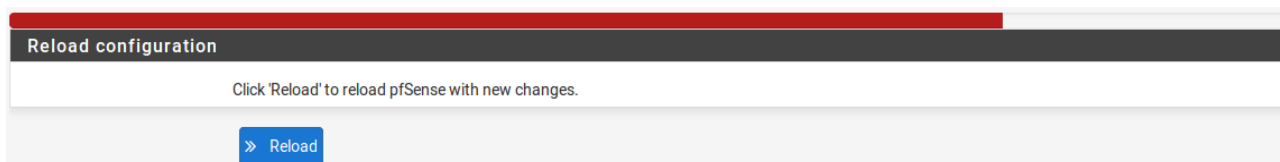
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

[Next](#)

Com isso terminamos o assistente inicial e podemos recarregar nosso servidor com as novas configurações clicando em Reload:

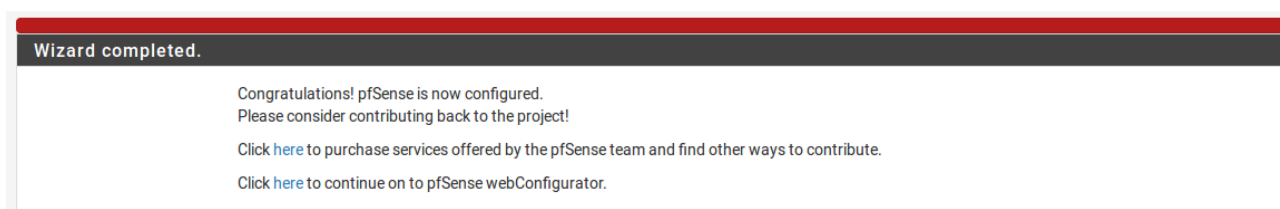


Reload configuration

Click 'Reload' to reload pfSense with new changes.

[Reload](#)

Será exibida uma mensagem notificando que as configurações foram finalizadas.



Wizard completed.

Congratulations! pfSense is now configured.
Please consider contributing back to the project!
Click [here](#) to purchase services offered by the pfSense team and find other ways to contribute.
Click [here](#) to continue on to pfSense webConfigurator.

Terminado o assistente de configuração inicial podemos acessar a página principal da interface de gerenciamento:

The screenshot displays the pfSense Status / Dashboard page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is divided into two panels: System Information and Interfaces.

System Information

| | |
|-------------------------|--|
| Name | firewall.multicorp.com.br |
| Version | 2.3.1-RELEASE (amd64) built on Tue May 17 18:46:53 CDT 2016 FreeBSD 10.3-RELEASE-p3 Version 2.3.1_1 is available. |
| Platform | pfSense |
| CPU Type | Intel(R) Core(TM) i7-3632QM CPU @ 2.20GHz |
| Uptime | 01 Hour 06 Minutes 51 Seconds |
| Current date/time | Thu Jun 9 16:12:21 BRT 2016 |
| DNS server(s) | • 127.0.0.1 • 10.10.2.94 |
| Last config change | Thu Jun 9 13:11:01 BRT 2016 |
| State table size | 0% (80/98000) Show states |
| MBUF Usage | 1% (760/61600) |
| Load average | 0.03, 0.01, 0.00 |
| CPU usage | 7% |
| Memory usage | 10% of 989 MiB |
| SWAP usage | 0% of 2047 MiB |
| Disk usage (/) | 10% of 5.8GiB - ufs |
| Disk usage (/var/run) | 2% of 3.4MiB - ufs in RAM |

Interfaces

| | | | |
|-----|---|-------------------------|------------|
| WAN | ↑ | 1000baseT <full-duplex> | 10.10.1.77 |
| LAN | ↑ | 1000baseT <full-duplex> | 10.10.2.12 |

Certificado https

Por padrão o PFSense redireciona seus acessos na porta http para a porta segura https porém como não temos um certificado válido, vamos configurá-lo para trabalhar na porta http e assim não receberemos alertas de segurança informando que nosso certificado não é válido.

Para isso Acessamos o menu System / Advanced e selecionamos a opção http ao invés de https

The screenshot displays the pfSense System / Advanced / Admin Access page. The top navigation bar includes links for System, Advanced, and Admin Access. The main content area is divided into two panels: Admin Access and webConfigurator.

Admin Access

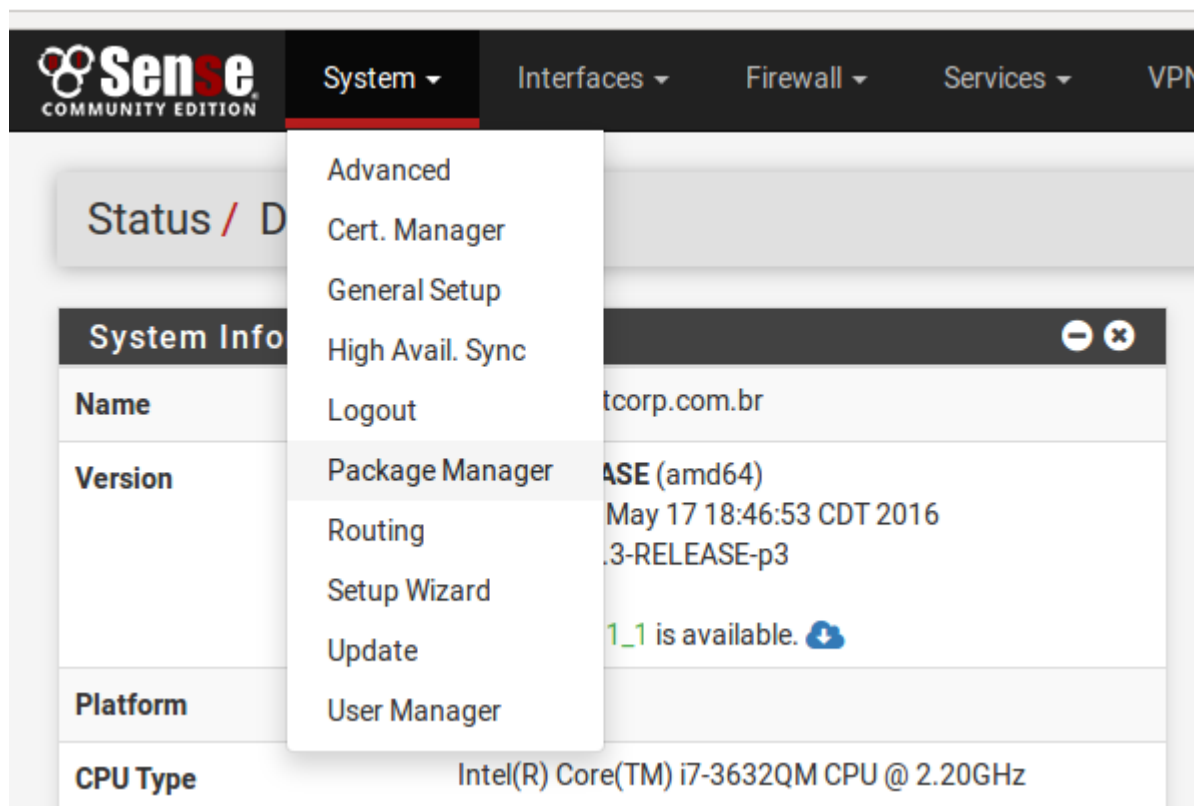
| | | | | | |
|--------------|----------------|------------|---------------|-----------------|---------------|
| Admin Access | Firewall & NAT | Networking | Miscellaneous | System Tunables | Notifications |
|--------------|----------------|------------|---------------|-----------------|---------------|

webConfigurator

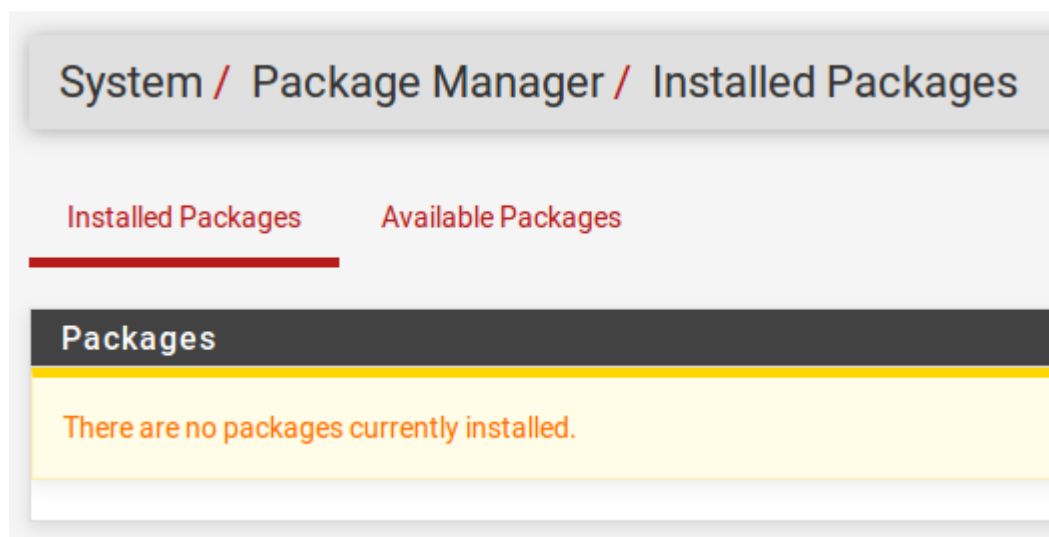
| | | |
|----------|---------------------------------------|-----------------------------|
| Protocol | <input checked="" type="radio"/> HTTP | <input type="radio"/> HTTPS |
|----------|---------------------------------------|-----------------------------|

Instalação dos pacotes nativos

Para a instalação dos pacotes nativos iremos utilizar o menu System / Package Manager:



A princípio não temos nenhum pacote instalado



Clique em Available Packages para selecionar os pacotes a serem instalados.

System / Package Manager / Available Packages

Installed Packages

Available Packages

Search

Search term

Both

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

| Name | Version | Description | |
|------------------|---------|--|-----------|
| arping | 1.2.2_1 | Broadcasts a who-has ARP packet on the network and prints answers. Package Dependencies: arping-2.15_1 | + Install |
| AutoConfigBackup | 1.45 | Automatically backs up your pfSense configuration. All contents are encrypted before being sent to the server. Requires Gold Subscription from pfSense Portal . | + Install |
| Avahi | 1.11_2 | Avahi is a system which facilitates service discovery on a local network via the mDNS/DNS-SD protocol suite. This enables you to plug your laptop or computer into a network and instantly be able to view other people who you can chat with, find printers to print to or find files being shared. In addition it supports some nifty things that have never been seen elsewhere like correct mDNS reflection across LAN segments. Compatible technology is found in Apple MacOS X (branded Bonjour and sometimes Zeroconf). Package Dependencies: avahi-app-0.6.31_5 | + Install |
| Backup | 0.4_1 | Tool to Backup and Restore files and directories. | + Install |
| bind | 9.10_8 | pfSense GUI for BIND DNS server Package Dependencies: bind-pfsense-9.10.3P4 | + Install |
| blinkled | 0.4.7_1 | Allows you to use LEDs for monitoring network activity on supported platforms (ALIX, WRAP, Soekris, etc.) Package Dependencies: blinkled-0.1 | + Install |

Squid

O primeiro pacote a ser instalado será o Squid Cache.

Utilizando o campo Search item podemos localizá-lo digitando squid como parâmetro de pesquisa.

System / Package Manager / Available Packages

Installed Packages

Available Packages

Search

Search term

squid

Both

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

| Name | Version | Description | |
|------------|---------|---|-----------|
| Lightsquid | 3.0.4 | LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid3 package. Package Dependencies: lightsquid-1.8_4 lighttpd-1.4.39_1 | + Install |
| squid | 0.4.18 | High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: squid_radius_auth-1.10 squid-3.5.19 squidclamav-6.14 c-icap-modules-0.4.2_1 | + Install |
| squidGuard | 1.14_3 | High performance web proxy URL filter. Package Dependencies: squidguard-1.4_15 | + Install |

O pacote em questão será o segundo, nesse caso squid 0.4.18. Basta clicar em Install.

System / Package Manager / Package Installer

Installed Packages

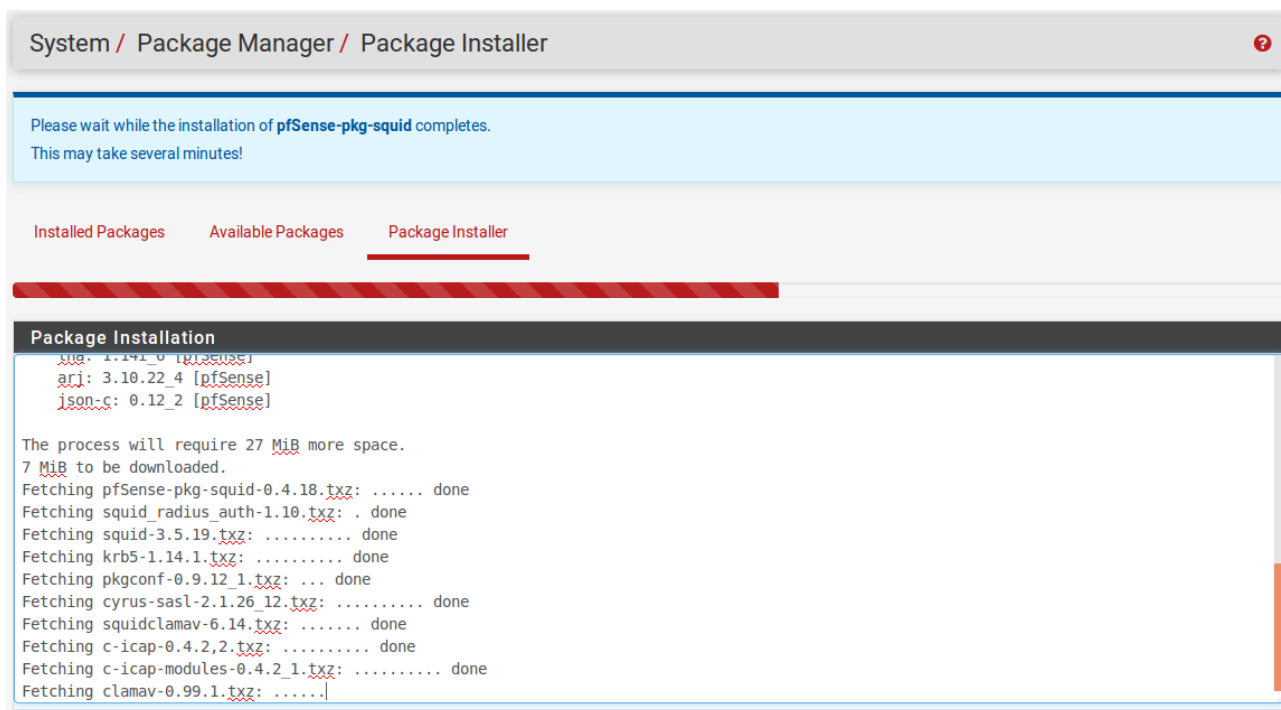
Available Packages

Package Installer

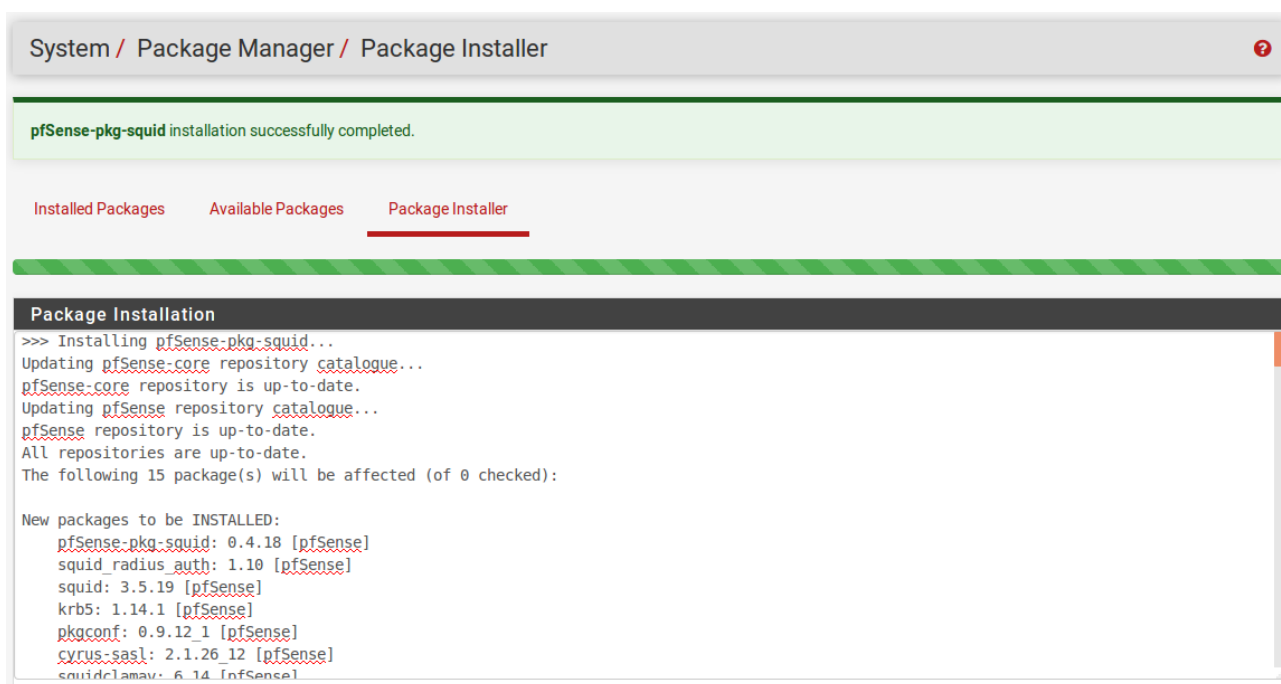
Confirmation Required to install package pfSense-pkg-squid.

Confirm

E confirmar a solicitação clicando em Confirm.



Aguarde até que a instalação seja concluída



A instalação também pode ser confirmada através da guia Installed Packages.








Perceba que ele já inclui o antivírus clamav e o módulo c-icap (responsável por fazer a conexão entre o proxy e o anti-vírus).




Installed Packages

Available Packages

Packages

Installed Packages

| Name | Category | Version | Description | Actions |
|--|----------|---------|---|---|
| ✓ squid | www | 0.4.18 | High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. |    |
| Package Dependencies: | | | | |
|  squid_radius_auth-1.10 | | | | |
|  squid-3.5.19 | | | | |
|  squidclamav-6.14 | | | | |
|  c-icap-modules-0.4.2_1 | | | | |

 = Update ✓ = Current = Remove  = Information  = Reinstall

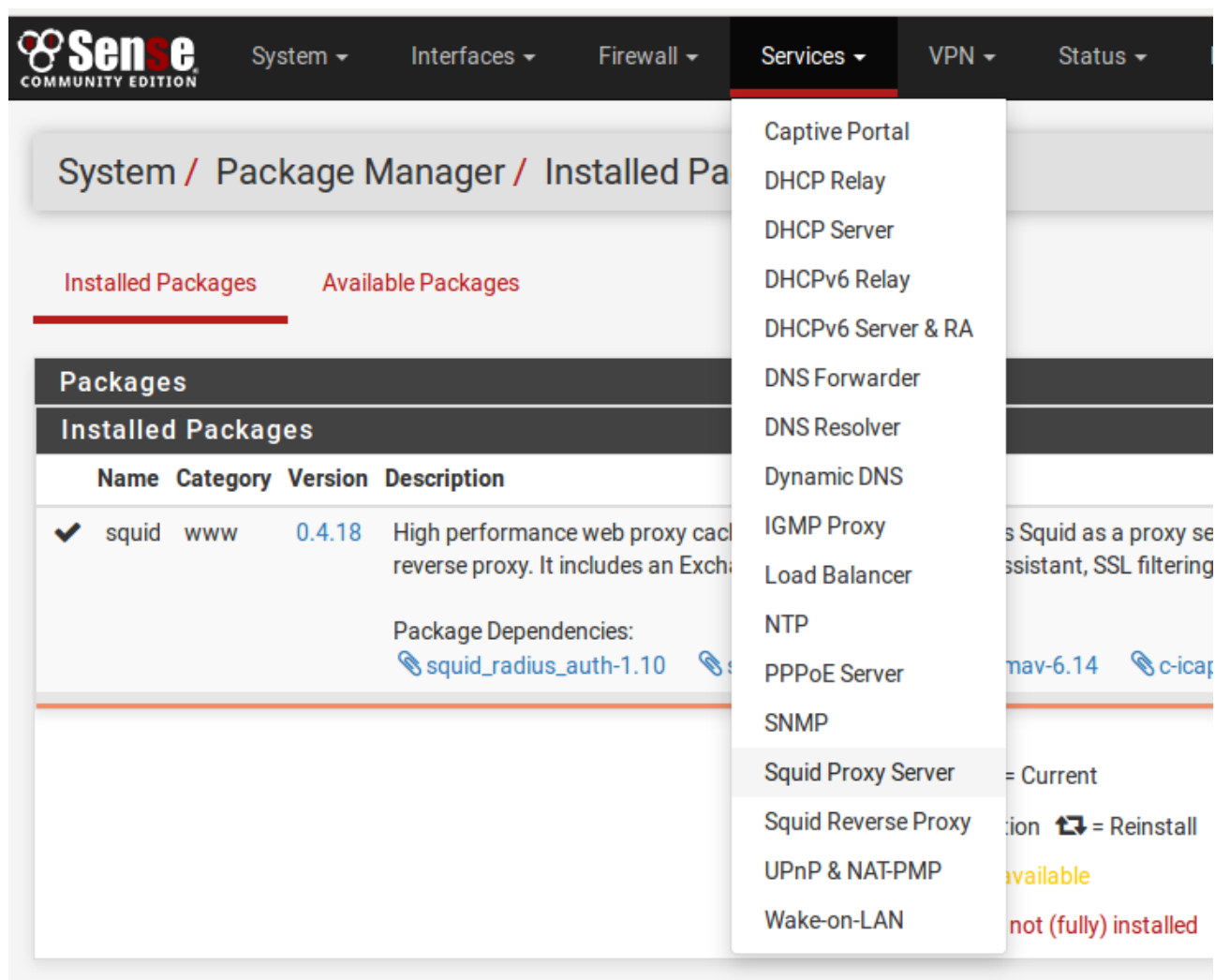
Newer version available

Package is configured but not (fully) installed

Ajustes Squid

Uma vez instalado vamos para as configurações.

As configurações básicas serão feitas pela própria interface através do menu Services / Squid Proxy Server



Será carregada a tela inicial de configuração do Squid na aba General.

Obs: Antes de começar os ajustes, é necessário acessar a aba Local Cache confirmar as opções clicando em Salvar no final da página. Não é necessário modificar nenhum parâmetro.

Em seguida voltamos às configurações partindo da aba General.

Package / Proxy Server: General Settings / General

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Sync

Squid General Settings

| | |
|--------------------------|--|
| Enable Squid Proxy | <input type="checkbox"/> Check to enable the Squid proxy. Note: If unchecked, ALL Squid services will be disabled and stopped. |
| Keep Settings/Data | <input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. Note: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade. |
| Proxy Interface(s) | <div>LAN WAN loopback</div> <p>The interface(s) the proxy server will bind to. Note: Use CTRL + click to select multiple interfaces.</p> |
| Proxy Port | <input type="text" value="3128"/> This is the port the proxy server will listen on. (Default: 3128) |
| ICP Port | <input type="text"/> This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP. |
| Allow Users on Interface | <input checked="" type="checkbox"/> If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets. |
| Patch Captive Portal | This feature was removed - see Bug #5594 for details! If you were using this feature, double-check '/etc/inc/captiveportal.inc' content for sanity. Get a sane copy of the file from pfSense GitHub repository if needed. |
| Resolve DNS IPv4 First | <input type="checkbox"/> Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites. |

Nesse formulário iremos ativar a serviço com a opção Enable Squid Proxy:

Enable Squid Proxy ☒ Check to enable the Squid proxy.
Note: If unchecked, ALL Squid services will be disabled and stopped.

Setar o endereço de listen (qual IP o serviço irá ouvir) para loopback, pois os usuários não poderão se conectar diretamente ao proxy, deverão se conectar ao Filtro de conteúdo Dansguardian.

Dessa forma apenas as requisições originadas do próprio servidor (o Dansguardian por exemplo) poderão se conectar ao proxy.

Proxy Interface(s)

LAN
WAN
loopback

The interface(s) the proxy server will bind to.
Note: Use CTRL + click to select multiple interfaces.

Para a aba General são apenas essas configurações, vamos então para a aba Antivirus:

Package / Proxy Server: Antivirus / Antivirus

General Remote Cache Local Cache **Antivirus** ACLs Traffic Mgmt Authentication Users Real Time Sync

ClamAV Anti-Virus Integration Using C-ICAP

Enable ☒ Enable Squid antivirus check using ClamAV.

Client Forward Options
Select what client info to forward to ClamAV.

Enable Manual Configuration
When enabled, the options below no longer have any effect.
You must edit the configuration files directly in the 'Advanced Features'.
Warning: Only enable this if you know what are you doing.
[Load Advanced](#) After enabling manual configuration, click this once to load default configuration files.
To disable manual configuration again, select 'disabled' and click 'Save'.

Redirect URL
When a virus is found then redirect the user to this URL.
Leave empty to use the default Squid/pfSense WebGUI URL.
Example: http://proxy.example.com/blocked.html

Google Safe Browsing ☐ Enables Google Safe Browsing support.
Google Safe Browsing database includes information about websites that may be phishing sites or possible sources of malware.
Note: This option consumes significant amount of RAM.
Important: Set 'ClamAV Database Update' below to 'every 1 hours' if you want to use this feature!

Exclude Audio/Video Streams ☐ This option disables antivirus scanning of streamed video and audio.

ClamAV Database Update
Optionally, you can schedule ClamAV definitions updates via cron.
Select the desired frequency here.
[Update AV](#) Click to update AV databases now.
Note: This will take a while. Check freshclam log on the 'Real Time' tab for progress information.

Como por padrão a checagem de vírus já vem ativado, devemos configurar apenas as opções:

ClamAVDatabase Update com o intervalo que acharmos mais conveniente, nessa ocasião foi escolhido de hora em hora.

ClamAV Database Update
Optionally, you can schedule ClamAV definitions updates via cron.
Select the desired frequency here.
[Update AV](#) Click to update AV databases now.
Note: This will take a while. Check freshclam log on the 'Real Time' tab for progress information.

Escolher uma localização para o mirror de atualização em Regional ClamAV Database Update Servers e por fim clicar em Salvar:

ClamAV Database Update

every 1 hours

Optionally, you can schedule ClamAV definitions updates via cron. Select the desired frequency here.

Update AV

Click to update AV databases now.

Note: This will take a while. Check freshclam log on the 'Real Time' tab for progress information.

Regional ClamAV Database Update Mirror

United States

Select regional database mirror.

Note: It is strongly recommended to choose something here and/or configure your own mirrors manually below. The default ClamAV database mirror performs extremely slow.

Optional ClamAV Database Update Servers

Enter ClamAV update servers here, or leave empty.

Note: For official update mirrors, use db.XY.clamav.net format. (Replace XY with your [country code](#).)

Note: Separate entries by semi-colons (;)

Save

Show Advanced Options

Obs.: Conforme indicado, o processo e os detalhes das atualizações podem ser conferidos na aba Real Time.

freshclam Table

ClamAV - freshclam Logs

Message

DON'T PANIC! Read <http://www.clamav.net/documents/upgrading-clamav>

WARNING: Local version: 0.99.1 Recommended version: 0.99.2

WARNING: Your ClamAV installation is OUTDATED!

ClamAV update process started at Thu Jun 9 17:00:44 2016

A próxima aba é a aba ACL.

Como faremos a filtragem de pacotes pelo Dansguardian, a única configuração necessária aqui é o parâmetro Allowed Subnets, onde deveremos setar as subredes que poderão ter acesso ao Proxy. Nessa ocasião 10.0.0.0/8.

Package / Proxy Server: Access Control / ACLs

General Remote Cache Local Cache Antivirus **ACLs** Traffic Mgmt Authentication Users Real Time Sync

Squid Access Control Lists

Allowed Subnets

10.0.0.0/8

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

Em seguida devemos configurar as autenticações, através da aba Authentication.

Temos diversas opções de autenticação conforme demonstra a imagem a seguir.

Local e LDAP são as opções mais comuns.

The screenshot shows the 'Squid Authentication General Settings' page. The breadcrumb trail is 'Package / Proxy Server: Authentication / Authentication'. The 'Authentication' tab is selected in the top navigation bar. The settings are as follows:

| Setting | Value |
|----------------------------|---|
| Authentication Method | None (dropdown menu open showing: None, Local, LDAP, RADIUS, Captive Portal, NT Domain) |
| Authentication Server | |
| Authentication server port | |

Below the 'Authentication server port' field, there is a note: 'Enter the port to use to connect to the authentication server here. Leave this field blank to use the authentication method's default port.'

Local, podemos criar os usuários localmente de forma bem simples através da aba Users, onde criamos um usuário chamado teste apenas para efetuarmos os testes posteriormente.

The screenshot shows the 'Proxy Server: Local Users / Users' page. The breadcrumb trail is 'Package / Proxy Server: Local Users / Users'. The 'Users' tab is selected in the top navigation bar. The page displays a table with the following data:

| Username | Description |
|----------|-------------|
| teste | |

Below the table, there is a green '+ Add' button. At the bottom left, there is a blue 'Save' button.

E LDAP seria para autenticação em um servidor OpenLDAP ou Microsoft Active Directory.

Veja no formulário mais abaixo que é possível setar todos os parâmetros LDAP de acordo com a base que for ser utilizada.

| Squid Authentication LDAP Settings | |
|------------------------------------|---|
| LDAP version | <input type="text" value="2"/> <small>Select LDAP protocol version.</small> |
| LDAP Server User DN | <input type="text"/> <small>Enter the user DN to use to connect to the LDAP server here.</small> |
| LDAP Password | <input type="password"/> <small>Enter the password to use to connect to the LDAP server here.</small> |
| LDAP Base Domain | <input type="text"/> <small>Enter the base domain of the LDAP server here.</small> |
| LDAP Username DN Attribute | <input type="text" value="uid"/> <small>Enter LDAP username DN attribute here.</small> |
| LDAP Search Filter | <input type="text" value="(&(objectClass=person)(uid=%s))"/> <small>Enter LDAP search filter here.</small> |

Obs.: Utilizaremos o método de autenticação local para os testes nessa ocasião.

Uma vez setado alguma forma de autenticação, todos os acessos deverão ser autenticados.

Caso haja necessidade de isentar alguma(s) estação(ões) de trabalho da necessidade de se autenticar, ainda na sessão inicial da aba Authentication (Squid Authentication General Settings) temos o campo: Subnets That Don't Need Authentication.

Basta cadastrar nesse campo os endereços com em formato CIDR conforme demonstra a imagem a seguir:

Subnets That Don't Need Authentication

Enter subnet(s) or IP address(es) (in CIDR format) that should NOT be asked for authentication to access the proxy.
Example (subnet): 10.5.0.0/16
Example (single host): 192.168.1.50/32

Note: Put each entry on a separate line.

Obs.:

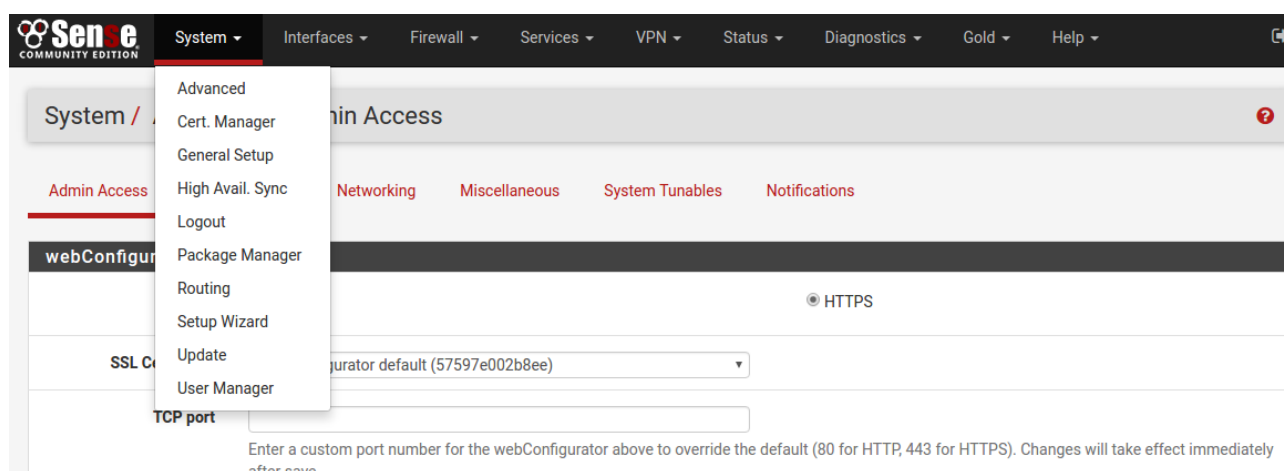
* Não será necessário configurar nada na aba ACLs pois não utilizaremos o Squid para filtragem de pacotes. Para essa finalidade será utilizado o Dansguardian, que possui uma interface de gerenciamento personalizada que abordaremos mais adiante.

* Não será possível utilizar o proxy ainda pois ele está ouvindo apenas no endereço de localhost que será para o Dansguardian.

Por fim faremos algumas modificações customizadas através do console para ajustar a questão de X_Forwarded_for e customizar as páginas de erros e de detecção de vírus.

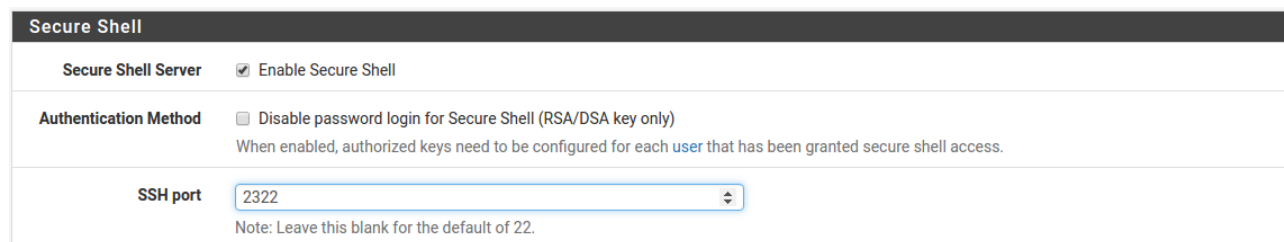
Para isso, antes de tudo, devemos ativar o serviço SSH no servidor para que possamos acessá-lo dessa forma.

Isso é feito através da opção Advanced do menu System.



Mais abaixo temos a sessão Secure Shell onde basta ativar o serviço através do Box Secure Shell Server.

Obs.: É recomendável alterar a porta padrão 22 para alguma outra porta desconhecida.



Feito isso podemos acessar o servidor para acesso via shell através do comando ssh com as credenciais do usuário admin (mesmo usuário de acesso à interface WEB).

Logo após o login é exibido o mesmo menu de opções que é exibido no console. Para acesso ao shell basta selecionar a opção 8.

```
fbuzon@fbuzon-Inspiron-7520:~$ ssh -p 2322 admin@10.10.2.12
Password for admin@firewall.multcorp.com.br:
*** Welcome to pfSense 2.3.1-RELEASE (amd64 full-install) on firewall ***

WAN (wan)      -> em0      -> v4: 10.10.1.77/24
LAN (lan)      -> em1      -> v4: 10.10.2.12/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 8

[2.3.1-RELEASE][admin@firewall.multcorp.com.br]/root: █
```

Temos o editor de texto ee (Easy Editor), nativo do FreeBSD e o vi versão antiga.

Caso prefira utilizar o editor vi moderno, podemos instalá-lo com o comando “pkg install vim-lite”.

```
[2.3.1-RELEASE][admin@firewall.multcorp.com.br]/usr/local/www: pkg install vim-lite
Updating pfSense-core repository catalogue...
pfSense-core repository is up-to-date.
Updating pfSense repository catalogue...
pfSense repository is up-to-date.
All repositories are up-to-date.
The following 1 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  vim-lite: 7.4.1556 [pfSense]

The process will require 22 MiB more space.
5 MiB to be downloaded.

Proceed with this action? [y/N]: y
Fetching vim-lite-7.4.1556.txz: 100%   5 MiB 375.4kB/s   00:14
Checking integrity... done (0 conflicting)
[1/1] Installing vim-lite-7.4.1556...
[1/1] Extracting vim-lite-7.4.1556: 100%
[2.3.1-RELEASE][admin@firewall.multcorp.com.br]/usr/local/www: █
```

Primeiro vamos ajustar a questão do X_Forwarded_for.

Para isso devemos criar uma ACL específica para localhost e aplicar a regra follow_x_forwarded_for nessa ACL através do squid.conf.

O arquivo de configuração squid.conf está localizado em /usr/local/etc/squid/squid.conf porém todas as modificações feitas diretamente nele são sobrescritas quando qualquer modificação é feita pela interface de gerenciamento.

Para que esses parâmetros sejam mantidos será necessário adicionar essas configurações no arquivo /usr/local/pkg/squid.inc.

Vamos editar esse arquivo então esse arquivo e localizar alterar o seguinte bloco:

```
# Setup some default acls
# From 3.2 further configuration cleanups have been done to make
# acl localhost src 127.0.0.1/32
acl allsrc src all
acl safeports port 21 70 80 210 280 443 488 563 591 631 777 901 {
acl sslports port 443 563 {$webgui_port} {$addtl_sslports}
```

Para:

```
# Setup some default acls
# From 3.2 further configuration cleanups have been done to make
acl localhost src 127.0.0.1/32
follow_x_forwarded_for allow localhost
acl allsrc src all
acl safeports port 21 70 80 210 280 443 488 563 591 631 777 901
acl sslports port 443 563 {$webgui_port} {$addtl_sslports}
```

Feito isso basta acessar a aba General do Serviço Squid Proxy Server e clicar em Salvar, não é necessário fazer nenhuma modificação, apenas clicar em salvar.

Nesso momento já podemos conferir no arquivo de configuração (/usr/local/etc/squid/squid.conf) que os parâmetros foram incorporados:

```
# Setup some default acls
# From 3.2 further configuration cleanups have been done to make things easier and safer.
acl localhost src 127.0.0.1/32
follow_x_forwarded_for allow localhost
acl allsrc src all
acl safeports port 21 70 80 210 280 443 488 563 591 631 777 901 3128 3129 1025-65535
acl sslports port 443 563
```

Vamos então instalar as páginas personalizadas de erros.

Esses arquivos estão localizados na pasta /usr/local/etc/squid/errors/en.

Basta entrar na pasta e baixar os arquivos diretamente do projeto no GitHub conforme demonstra a imagem a seguir:

https://github.com/fernandobuzon/dansguardianAdmin/raw/master/custom_squid_erros.tar.gz

```
[2.3.1-RELEASE] [admin@firewall.multcorp.com.br]/root: cd /usr/local/etc/squid/errors/en
[2.3.1-RELEASE] [admin@firewall.multcorp.com.br]/usr/local/etc/squid/errors/en: fetch https://github.com/fernandobuzon/dansguardianAdmin/raw/master/custom_squid_erros
.tar.gz
custom_squid_erros.tar.gz          100% of 20 kB 106 kBps 00m00s
[2.3.1-RELEASE] [admin@firewall.multcorp.com.br]/usr/local/etc/squid/errors/en: tar zxvf custom_squid_erros.tar.gz
x ERR_ACCESS_DENIED
x ERR_CONNECT_FAIL
x ERR_DNS_FAIL
x ERR_FTP_FAILURE
x ERR_FTP_FORBIDDEN
x ERR_FTP_NOT_FOUND
[2.3.1-RELEASE] [admin@firewall.multcorp.com.br]/usr/local/etc/squid/errors/en: █
```

Exemplo de página não encontrada:



A URL requisitada não pôde ser reperada

O seguinte erro foi encontrado ao tentar recuperar a URL:

<http://naoexiste.nao/>

Impossível determinar o endereço IP do nome de host "naoexiste.nao"

O servidor DNS retornou:

Name Error: The domain name does not exist.

Isto significa que o cache não pode resolver o nome de host contido na URL. Verifique se o endereço está correto.

Em caso de dúvidas, favor entrar em contato com o departamento de TI pelo email suporte@multcorp.com.br.

Powered by [MultCorp](#)

Também iremos personalizar a página de alerta de Vírus, localizada em /usr/local/www/squid_clwarn.php.

https://github.com/fernandobuzon/dansguardianAdmin/raw/master/squid_clwarn.php

```
[2.3.1-RELEASE] admin@firewall.multcorp.com.br /root: cd /usr/local/www/
[2.3.1-RELEASE] admin@firewall.multcorp.com.br /usr/local/www: fetch https://github.com/fernandobuzon/dansguardianAdmin/raw/master/squid_clwarn.php
squid_clwarn.php 100% of 24 kB 147 kBps 00m00s
[2.3.1-RELEASE] admin@firewall.multcorp.com.br /usr/local/www: █
```

Exemplo de aviso de vírus:



Vírus Detectado!

Foi identificado um vírus na URL requisitada:

<http://www.eicar.org/download/eicar.com>

Vírus encontrado: stream: Eicar-Test-Signature FOUND

Origem da requisição: 10.10.2.10 teste

Em caso de dúvidas, favor entrar em contato com o departamento de TI pelo email suporte@multcorp.com.br.

Powered by [MultCorp](#)

Obs.: Para não ter problema de acesso à image do logotipo, ela está de forma embed via base64 nos próprios arquivos.

Para alterar o logotipo basta gerar um base64 da nova imagem e substituir logo no começo dos arquivos na TAG img:

```
<html>

<head>
<title>MultCorp - Acesso negado</title>
<meta charset="UTF-8">
</head>

<body bgcolor=#FFFFFF>

<center>
<img src="data:image/png;base64,iVBORw0KGgoAAAANSUheEU
```

Com isso terminamos a configuração do Squid.

Instalação dos pacotes Pré-Compilados

O PFSense por padrão não possui compilador e seguindo as recomendação do próprio projeto, é recomendado que aplicações customizadas sejam compiladas a parte em um outro computador com o mesmo Kernel, FreeBSD.

Can I compile software on pfSense

Q: Can I compile software on pfSense in the shell or console?

The short answer: No

The long answer: No, because pfSense intentionally does not include a proper environment for compiling software (make, headers/includes, sources, etc) on the installed firewall. Those tools are left out for security and capacity reasons.

A virtual machine or separate system can be setup to compile software, and then the compiled binaries/packages/software can be moved over to the firewall.

When doing this, install a version of FreeBSD that matches up with the version of pfSense currently in use. A list can be found here: [Versions of pfSense and FreeBSD](#)

Alternately, install pre-compiled FreeBSD packages as described here: [Installing FreeBSD Packages](#)

Categories: [FAQ](#) | [FreeBSD](#) | [Packages](#)

Tanto o Dansguardian como o Sarg foram compilados em um servidor FreeBSD 10.3 a parte.

Dansguardian

O Dansguardian por ter sido removido o Ports do FreeBSD, foi compilado a partir de sua última versão estável disponibilizada no SourceForge:

<https://sourceforge.net/projects/dansguardian/files/>

Após a compilação, os arquivos foram ajustados de uma forma específica para trabalhar com sua interface de gerenciamento e os arquivos estão disponíveis no GitHub através da seguinte URL:

<https://github.com/fernandobuzon/dansguardianAdmin/raw/master/dansguardian-2.12.00.tar.gz>

Obs.: Os arquivos já estão organizados quanto à hierarquia de pastas e devem ser extraídos a partir da pasta raiz do sistema “/”.

```
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]: fetch https://github.com/fernandobuzon/dansguardianAdmin/raw/master/dansguardian-2.12.00.tar.gz
dansguardian-2.12.00.tar.gz 100% of 2009 kB 50 kBps 00m40s
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]: tar zxvf dansguardian-2.12.00.tar.gz
```

```
x usr/local/etc/dansguardian/lists/install/weightedphraselist
x usr/local/etc/dansguardian/lists/install/picsfile
x usr/local/etc/dansguardian/lists/default/picsfile
x usr/local/etc/dansguardian/lists/default/bannedextensionlist
x usr/local/etc/dansguardian/lists/default/bannedmimetyplist
x usr/local/etc/dansguardian/lists/default/bannedphraselist
x usr/local/etc/dansguardian/lists/default/bannedregexheaderlist
x usr/local/etc/dansguardian/lists/default/bannedregexpurllist
x usr/local/etc/dansguardian/lists/default/bannedsitelist
x usr/local/etc/dansguardian/lists/default/bannedurllist
x usr/local/etc/dansguardian/lists/default/contentregexplist
x usr/local/etc/dansguardian/lists/default/exceptionextensionlist
x usr/local/etc/dansguardian/lists/default/exceptionfilesitelist
x usr/local/etc/dansguardian/lists/default/exceptionfileurllist
x usr/local/etc/dansguardian/lists/default/exceptionmimetyplist
x usr/local/etc/dansguardian/lists/default/exceptionphraselist
x usr/local/etc/dansguardian/lists/default/exceptionregexpurllist
x usr/local/etc/dansguardian/lists/default/exceptionsitelist
x usr/local/etc/dansguardian/lists/default/exceptionurllist
x usr/local/etc/dansguardian/lists/default/greysitelist
x usr/local/etc/dansguardian/lists/default/greyurllist
x usr/local/etc/dansguardian/lists/default/headerregexplist
x usr/local/etc/dansguardian/lists/default/logregexpurllist
x usr/local/etc/dansguardian/lists/default/logsitelist
x usr/local/etc/dansguardian/lists/default/logurllist
x usr/local/etc/dansguardian/lists/default/urlregexplist
x usr/local/etc/dansguardian/lists/default/weightedphraselist
x usr/local/etc/dansguardian/lists/default/weightedphraselist.bkp
x usr/local/etc/dansguardian/downloadmanagers/default.conf
x usr/local/etc/dansguardian/downloadmanagers/fancy.conf
x usr/local/etc/dansguardian/bannedrooms/default
x usr/local/etc/dansguardian/authplugins/proxy-basic.conf
x usr/local/etc/dansguardian/authplugins/ident.conf
x usr/local/etc/dansguardian/authplugins/ip.conf
x usr/local/etc/dansguardian/authplugins/proxy-digest.conf
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]:
```


Após a extração dos arquivos do Dansguardian propriamente dito vamos baixar sua interface de gerenciamento na pasta /usr/local/www/filtro.

<https://github.com/fernandobuzon/dansguardianAdmin/archive/master.zip>

```
[2.3.1-RELEASE] [admin@firewall.multicorp.com.br]: cd /usr/local/www
[2.3.1-RELEASE] [admin@firewall.multicorp.com.br]: /usr/local/www: mkdir filtro
[2.3.1-RELEASE] [admin@firewall.multicorp.com.br]: /usr/local/www: cd filtro
[2.3.1-RELEASE] [admin@firewall.multicorp.com.br]: /usr/local/www/filtro: fetch https://github.com/fernandobuzon/dansguardianAdmin/archive/master.zip
master.zip
100% of 3571 kB 882 kBps 00m04s
[2.3.1-RELEASE] [admin@firewall.multicorp.com.br]: /usr/local/www/filtro: unzip master.zip
Archive: master.zip
d dansguardianAdmin-master
  extracting: dansguardianAdmin-master/README
  extracting: dansguardianAdmin-master/ac_add.php
  extracting: dansguardianAdmin-master/ac_del.php
  extracting: dansguardianAdmin-master/ac_edit.php
  extracting: dansguardianAdmin-master/ac_status.php
  extracting: dansguardianAdmin-master/ac_weight.php
  extracting: dansguardianAdmin-master/add.php
  extracting: dansguardianAdmin-master/confdel.php
  extracting: dansguardianAdmin-master/config.php
  extracting: dansguardianAdmin-master/custom_squid_errros.tar.gz
  extracting: dansguardianAdmin-master/dansguardian-2.12.00.tar.gz
  extracting: dansguardianAdmin-master/edit.php
  extracting: dansguardianAdmin-master/filter.php
  extracting: dansguardianAdmin-master/index.php
  extracting: dansguardianAdmin-master/logo.png
  extracting: dansguardianAdmin-master/sarg-2.3.9.tar.gz
  extracting: dansguardianAdmin-master/squid_clwarn.php
[2.3.1-RELEASE] [admin@firewall.multicorp.com.br]: /usr/local/www/filtro: mv dansguardianAdmin-master/* .
[2.3.1-RELEASE] [admin@firewall.multicorp.com.br]: /usr/local/www/filtro: █
```

Agora iremos adicionar a opção Filtro WEB ao menu de Serviços do PFSense através do arquivo /usr/local/www/head.inc.

Localize o bloco \$Services_menu[] e adicione ao final uma linha conforme demonstrado na imagem.

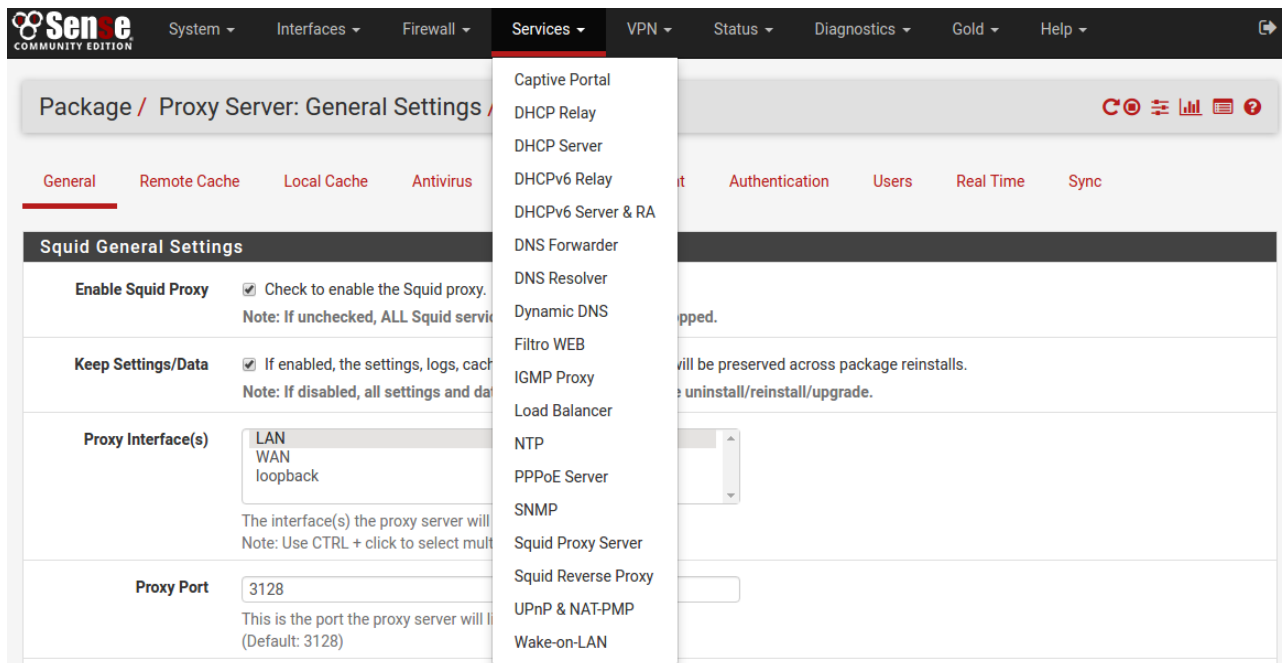
```
$services_menu[] = array(gettext("Filtro WEB"), "/filtro/index.php");
```

```
// Services
$services_menu = array();
$services_menu[] = array(gettext("Captive Portal"), "/services_captiveportal.php");
$services_menu[] = array(gettext("DNS Forwarder"), "/services_dnsmasq.php");
$services_menu[] = array(gettext("DNS Resolver"), "/services_unbound.php");
$services_menu[] = array(gettext("DHCP Relay"), "/services_dhcp_relay.php");
$services_menu[] = array(gettext("DHCPv6 Relay"), "/services_dhcpv6_relay.php");

if ($g['services_dhcp_server_enable']) {
    $services_menu[] = array(gettext("DHCP Server"), "/services_dhcp.php");
    $services_menu[] = array(htmlspecialchars(gettext("DHCPv6 Server & RA")), "/services_dhcpv6.php");
}

$services_menu[] = array(gettext("Dynamic DNS"), "/services_dyndns.php");
$services_menu[] = array(gettext("IGMP Proxy"), "/services_igmpproxy.php");
$services_menu[] = array(gettext("Load Balancer"), "/load_balancer_pool.php");
$services_menu[] = array(gettext("NTP"), "/services_ntpd.php");
$services_menu[] = array(gettext("PPPoE Server"), "/services_pppoe.php");
$services_menu[] = array(gettext("SNMP"), "/services_snmp.php");
$services_menu[] = array(gettext("Filtro WEB"), "/filtro/index.php");
```

Após isso basta atualizar a página e conferir a nova opção no menu:



Por final devemos criar a pasta de Log e setar seus owner para nobody:

```
mkdir -p /usr/local/var/log/dansguardian
```

```
chown nobody /usr/local/var/log/dansguardian
```

```
[2.3.1-RELEASE] [admin@firewall.multicorp.com.br]: mkdir -p /usr/local/var/log/dansguardian
[2.3.1-RELEASE] [admin@firewall.multicorp.com.br]: chown nobody /usr/local/var/log/dansguardian
```

E para encerrar com o Dansguardian resta apenas configurar para que o mesmo seja inicializado automaticamente durante o boot.

Seguindo o padrão do PFSense, basta copiar o seu arquivo de inicialização para a pasta correta:

```
cp /usr/local/share/dansguardian/scripts/bsd-init /usr/local/etc/rc.d/dansguardian.sh
```

```
chmod +x /usr/local/etc/rc.d/dansguardian.sh
```

```
/: cp /usr/local/share/dansguardian/scripts/bsd-init /usr/local/etc/rc.d/dansguardian.sh
/: chmod +x /usr/local/etc/rc.d/dansguardian.sh
```

Agora basta acessar a interface de gerenciamento do Filtro WEB através da opção recém adicionada ao menu para iniciar o serviço e gerenciá-lo.

Apesar de ser possível acessar diretamente essa interface adicionando ao final da URL de aceso ao PFSense a pasta /filtro, será verificada a autenticação do usuário no PFSense e caso não esteja autenticado será redirecionado para a página de autenticação.

Abaixo temos uma imagem da página inicial da interface de gerenciamento de filtragem:



Status: Rodando.

Parar

Recarregar

Reiniciar

Exceções por IP

Exceções por Usuário

Grupos de Filtragem:

default

Editar

Novo Grupo

Voltar

Sarg

O Sarg, assim como o Dansguardian, também foi compilado em um servidor a parte, porém como ainda está com o projeto ativo, foi compilado via Ports.

Seus binários assim como as bibliotecas necessárias para o seu funcionamento também estão disponíveis no projeto.

Basta baixar o arquivo compactado e extrair a partir da pasta raiz “/”.

<https://github.com/fernandobuzon/dansguardianAdmin/raw/master/sarg-2.3.9.tar.gz>

```
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]: fetch https://github.com/fernandobuzon/dansguardianAdmin/raw/master/sarg-2.3.9.tar.gz
sarg-2.3.9.tar.gz 100% of 1524 kB 454 kBps 00m04s

x usr/local/etc/sarg/sarg-php/locale/ru/
x usr/local/etc/sarg/sarg-php/locale/ru/LC_MESSAGES/
x usr/local/etc/sarg/sarg-php/locale/ru/LC_MESSAGES/messages.mo
x usr/local/etc/sarg/sarg-php/locale/ru/LC_MESSAGES/messages.po
x usr/local/etc/sarg/sarg-php/locale/pt_BR/LC_MESSAGES/
x usr/local/etc/sarg/sarg-php/locale/pt_BR/LC_MESSAGES/messages.mo
x usr/local/etc/sarg/sarg-php/locale/pt_BR/LC_MESSAGES/messages.po
x usr/local/etc/sarg/sarg-php/locale/fr/LC_MESSAGES/
x usr/local/etc/sarg/sarg-php/locale/fr/LC_MESSAGES/messages.mo
x usr/local/etc/sarg/sarg-php/locale/fr/LC_MESSAGES/messages.po
x usr/local/etc/sarg/sarg-php/locale/en_EN/LC_MESSAGES/
x usr/local/etc/sarg/sarg-php/locale/en_EN/LC_MESSAGES/messages.mo
x usr/local/etc/sarg/sarg-php/locale/en_EN/LC_MESSAGES/messages.po
x usr/local/etc/sarg/images/datetime.png
x usr/local/etc/sarg/images/graph.png
x usr/local/etc/sarg/images/sarg-squidguard-block.png
x usr/local/etc/sarg/images/sarg.png
x usr/local/etc/sarg/fonts/DejaVuSans.ttf
x usr/local/etc/sarg/fonts/FreeSans.ttf
x usr/local/etc/sarg/fonts/README
x usr/local/etc/sarg/fonts/license
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]: █
```

Após extraídos os arquivos, devemos agendar via crontab a geração dos relatórios através do comando:

crontab -e

Será aberto o editor de texto vim onde devemos adicionar a seguinte linha de dados:

* /5 * * * * /usr/local/bin/php /usr/local/etc/sarg/sarg.php > /dev/null

Saia e salve digitando: “:wq”

Obs.: Perceba que o arquivo executado não é o binário do Sarg propriamente, mas sim um arquivo .php. Esse arquivo é o responsável por executar o binário de fato e tratar o arquivo gerado na questão de atualizar o logotipo (necessário fazer a cada geração de um novo relatório) e exigir a autenticação do PFSense para o seu acesso.

E para concluir com o Sarg, vamos também adicioná-lo ao menu, também através do arquivo /usr/local/www/head.inc, porém dessa vez utilizaremos o menu status.

Edite o arquivo e localize o bloco \$status_menu[] e adicione uma linha no final:

```
$status_menu[] = array(gettext("Filter Report"), "/sarg/");
```

```
// Status
$status_menu = array();
$status_menu[] = array(gettext("Captive Portal"), "/status_captiveportal.php");
$status_menu[] = array(gettext("CARP (failover)"), "/status_carp.php");
$status_menu[] = array(gettext("Dashboard"), "/index.php");
$status_menu[] = array(gettext("Gateways"), "/status_gateways.php");
$status_menu[] = array(gettext("DHCP Leases"), "/status_dhcp_leases.php");
$status_menu[] = array(gettext("DHCPv6 Leases"), "/status_dhcpv6_leases.php");
$status_menu[] = array(gettext("Filter Reload"), "/status_filter_reload.php");
$status_menu[] = array(gettext("Interfaces"), "/status_interfaces.php");
$status_menu[] = array(gettext("IPsec"), "/status_ipsec.php");
$status_menu[] = array(gettext("Load Balancer"), "/status_lb_pool.php");
$status_menu[] = array(gettext("NTP"), "/status_ntpd.php");
$status_menu[] = array(gettext("OpenVPN"), "/status_openvpn.php");

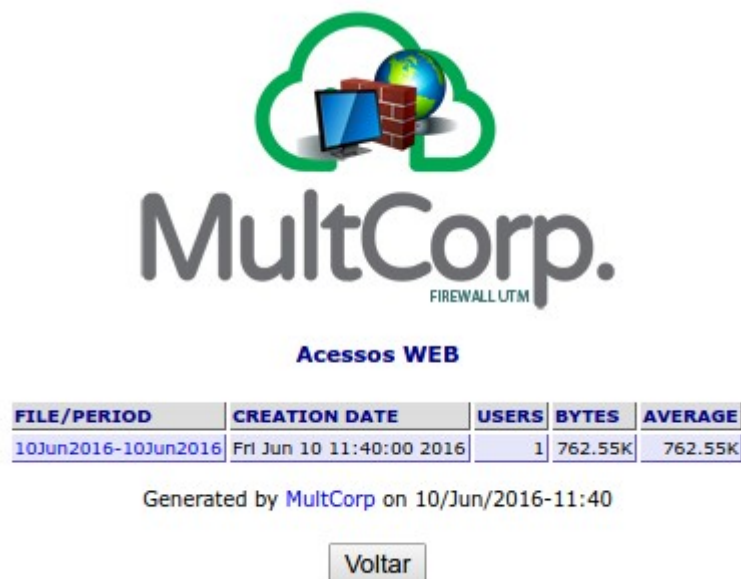
if ($g['platform'] == $g['product_name']) {
    $status_menu[] = array(gettext("Package Logs"), "/status_pkglogs.php");
}

$status_menu[] = array(gettext("Queues"), "/status_queues.php");
$status_menu[] = array(gettext("Services"), "/status_services.php");
$status_menu[] = array(gettext("System Logs"), "/status_logs.php");
$status_menu[] = array(gettext("Traffic Graph"), "/status_graph.php?if=wan");
$status_menu[] = array(gettext("Filter Report"), "/sarg/");
```

Basta recarregar a página para conferir a nova opção no menu:

The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', 'Gold', and 'Help'. The 'Status' menu is open, displaying a list of options: Captive Portal, CARP (failover), Dashboard, DHCP Leases, DHCPv6 Leases, Filter Reload, Filter Report, Gateways, Interfaces, IPsec, Load Balancer, Monitoring, NTP, OpenVPN, Package Logs, Queues, Services, System Logs, Traffic Graph, and UPnP & NAT-PMP. The 'Filter Report' option is highlighted. On the left, the 'System Information' panel is visible, showing details like Name (firewall.multicorp.com.br), Version (2.3.1-RELEASE), Platform (pfSense), CPU Type (Intel(R) Core(TM) i7-3632QM CPU @ 2.20GHz), Uptime (03 Hours 04 Minutes 16 Seconds), Current date/time (Fri Jun 10 11:38:56 BRT 2016), DNS server(s) (127.0.0.1, 10.10.2.94), Last config change (Fri Jun 10 11:16:53 BRT 2016), State table size (0% (86/98000)), MBUF Usage (2% (1266/61600)), and Load average (0.15, 0.04, 0.01).

E a seguir temos a tela inicial do relatório gerado:



DHCP Server

Para atribuição automática de IP para as estação devemos ativar o serviço de DHCP através do menu Services / DHCP Server.

Para isso basta marcar o Box Enable logo no início.

Services / DHCP Server / LAN

WAN LAN

General Options

| | |
|-----------------------|---|
| Enable | <input checked="" type="checkbox"/> Enable DHCP server on LAN interface |
| Deny unknown clients | <input type="checkbox"/> Only the clients defined below will get DHCP leases from this server. |
| Ignore denied clients | <input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured. |
| Subnet | 10.10.2.0 |
| Subnet mask | 255.255.255.0 |
| Available range | 10.10.2.1 - 10.10.2.254 |
| Range | <input type="text" value="10.10.2.21"/> <input type="text" value="10.10.2.245"/> From To |

Além de ativar o serviço, é necessário configurar pelo menos os seguintes parâmetros na Sessão Other Options:

| Other Options | |
|---------------|---|
| Gateway | <input type="text" value="10.10.2.12"/> <small>The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.</small> |
| Domain name | <input type="text" value="multicorp.com.br"/> <small>The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.</small> |

Configuração automática do Proxy

Para finalizarmos todo o processo vamos configurar o servidor DNS para que as estações possam reconhecer o proxy de forma automática e dessa forma não seja necessário configurá-lo individualmente nas estações de trabalho.

Para isso criaremos na pasta /usr/local/www um arquivo chamado wpad.dat com o seguinte conteúdo:

```
function FindProxyForURL(url,host)
{
return "PROXY 10.10.2.12:8080";
}
```

Obs.: Substitua o IP 10.10.2.12 pelo IP correto do servidor na interface LAN.

Alguns browsers tentam localizar arquivos com outros nomes e então criaremos alguns links simbólicos para esses nomes distintos apontando para o mesmo arquivo:

```
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]: cd /usr/local/www
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]/usr/local/www: echo 'function FindProxyForURL(url,host)' > wpad.dat
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]/usr/local/www: echo '{' >> wpad.dat
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]/usr/local/www: echo 'return "PROXY 10.10.2.12:8080";' >> wpad.dat
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]/usr/local/www: echo '}' >> wpad.dat
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]/usr/local/www: ln -s wpad.dat wpad.da
[2.3.1-RELEASE][admin@firewall.multicorp.com.br]/usr/local/www: ln -s wpad.dat proxy.pac
```

Agora temos que criar um registro no servidor DNS para o host:

wpad.multicorp.com.br

Obs.: O host deve ser wpad. O nome do domínio que estivermos configurado no servidor DHCP.

Faremos essa configuração utilizando o Serviço DNS Forwarder porém antes disso será necessário desativarmos, por questões de conflito, o serviço DNS Resolver.

Basta acessar o menu Services / DNS Resolver e desmarcar a opção Enable DNS resolver:

Services / DNS Resolver / General Settings

General Settings Advanced Settings Access Lists

General DNS Resolver Options

Enable ☐ Enable DNS resolver

Save

Em seguida vamos no menu Services / DNS Forwarder.

Clique em + Add na sessão Host Overrides.

| Host Overrides | | | | |
|----------------|--------|----|-------------|---------|
| Host | Domain | IP | Description | Actions |
| | | | | |
| | | | | |

+ Add

Crie o registro apontando para o IP do servidor na rede LAN:

Services / DNS Forwarder / Edit Host Override

Host Override Options

Host
Name of the host, without the domain part
e.g.: "myhost"

Domain
Domain of the host
e.g.: "example.com"

IP Address
IP address of the host
e.g.: 192.168.100.100 or fd00:abcd::1

Description
A description may be entered here for administrative reference (not parsed).

E ative o serviço marcando a opção Enable DNS forwarder:

Services / DNS Forwarder

General DNS Forwarder Options

Enable ☒ Enable DNS forwarder

A partir desse momento, estações que estiverem com a configuração de proxy setada para detecção automática de proxy, irão reconhecer e utilizar o servidor.

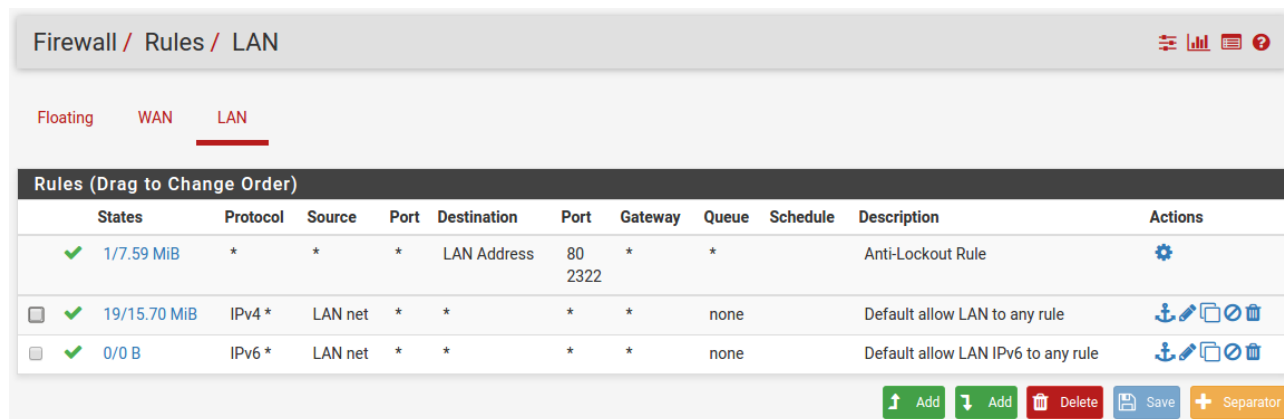
Caso queiramos, propositalmente, excluir alguma estação de passar pelo proxy, ele deverá ser configurada manualmente para não utilizar proxy.

Bloqueio de acessos por fora do Proxy

Como dito no tópico anterior, as estações detectarão e utilizarão o proxy de forma automática, porém nada impede o usuário de setar sua própria estação de trabalho para não utilizar proxy e fazer seus acessos diretamente.

O bloqueio desses acessos deve ser feito através do Firewall.

Para acessar e gerenciar as regras de Firewall utilizaremos o menu Firewall / Rules na aba LAN.



The screenshot shows the Mikrotik WinBox interface for configuring Firewall Rules. The breadcrumb navigation at the top reads "Firewall / Rules / LAN". Below this, there are tabs for "Floating", "WAN", and "LAN", with "LAN" being the active tab. The main area displays a table of rules with the title "Rules (Drag to Change Order)". The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are three rules listed: 1. "Anti-Lockout Rule" with a green status icon, 1/7.59 MiB, protocol *, source *, port *, destination "LAN Address", port "80 2322", gateway *, queue *, and description "Anti-Lockout Rule". 2. "Default allow LAN to any rule" with a green status icon, 19/15.70 MiB, protocol "IPv4 *", source "LAN net", port *, destination *, gateway *, queue "none", and description "Default allow LAN to any rule". 3. "Default allow LAN IPv6 to any rule" with a green status icon, 0/0 B, protocol "IPv6 *", source "LAN net", port *, destination *, gateway *, queue "none", and description "Default allow LAN IPv6 to any rule". At the bottom right, there are buttons for "Add", "Add", "Delete", "Save", and "Separator".

| Rules (Drag to Change Order) | | | | | | | | | | |
|------------------------------|----------|---------|------|-------------|---------|---------|-------|----------|------------------------------------|-----------|
| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| ✓ 1/7.59 MiB | * | * | * | LAN Address | 80 2322 | * | * | | Anti-Lockout Rule | ⚙️ |
| ☐ ✓ 19/15.70 MiB | IPv4 * | LAN net | * | * | * | * | none | | Default allow LAN to any rule | 📌 🖋️ 📄 🗑️ |
| ☐ ✓ 0/0 B | IPv6 * | LAN net | * | * | * | * | none | | Default allow LAN IPv6 to any rule | 📌 🖋️ 📄 🗑️ |

Essas são as regras default, criaremos mais duas regras acima da regra número 2.

Nessas regras iremos bloquear os acessos da interface LAN, originados de qualquer IP que não seja o IP do próprio servidor com destino a qualquer endereço nas portas 80 (http) e 443 (https).

Uma regra para os acessos http:

| Edit Firewall Rule | |
|-------------------------------|--|
| Action | <div>Block</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</div> |
| Disabled | <div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div> |
| Interface | <div>LAN</div> <div>Choose the interface from which packets must come to match this rule.</div> |
| Address Family | <div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div> |
| Protocol | <div>TCP</div> <div>Choose which IP protocol this rule should match.</div> |
| Source | |
| Source | <div><input checked="" type="checkbox"/> Invert match.</div> <div>LAN address</div> <div>Source Address /</div> |
| Display Advanced | <div>Display Advanced</div> |
| Destination | |
| Destination | <div><input type="checkbox"/> Invert match.</div> <div>any</div> <div>Destination Address /</div> |
| Destination port range | <div>HTTP (80)</div> <div>From Custom To Custom</div> <div>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</div> |
| Extra Options | |
| Log | <div><input type="checkbox"/> Log packets that are handled by this rule</div> <div>Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).</div> |
| Description | <div>Bloqueio de acessos http for do proxy</div> <div>A description may be entered here for administrative reference.</div> |
| Advanced Options | <div>Display Advanced</div> |

E outra regra para os acessos https:

Edit Firewall Rule

Action

Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

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

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☒ Invert match.

LAN address

Source Address

/

Display Advanced

Display Advanced

Destination

Destination

☐ Invert match.

any

Destination Address

/

Destination port range

HTTPS (443)

From

Custom

To

HTTPS (443)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Bloqueio de acessos https para do proxy

A description may be entered here for administrative reference.

Advanced Options

Display Advanced

Por fim aplicar a nova configuração clicando em Apply Changes.

Firewall / Rules / LAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating

WAN

LAN

Rules (Drag to Change Order)

| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|--------------------------|---------------|----------|---------------|------|-------------|-------------|---------|-------|----------|---|---------|
| | ✓ 0/8.33 MiB | * | * | * | LAN Address | 80 2322 | * | * | | Anti-Lockout Rule | ⚙ |
| <input type="checkbox"/> | ✗ 0/0 B | IPv4 TCP | ! LAN address | * | * | 80 (HTTP) | * | none | | Bloqueio de acessos http para do proxy | ⚙🔗🗑🔒🗑 |
| <input type="checkbox"/> | ✗ 0/0 B | IPv4 TCP | ! LAN address | * | * | 443 (HTTPS) | * | none | | Bloqueio de acessos https para do proxy | ⚙🔗🗑🔒🗑 |
| <input type="checkbox"/> | ✓ 8/15.90 MiB | IPv4 * | LAN net | * | * | * | * | none | | Default allow LAN to any rule | ⚙🔗🗑🔒🗑 |
| <input type="checkbox"/> | ✓ 0/0 B | IPv6 * | LAN net | * | * | * | * | none | | Default allow LAN IPv6 to any rule | ⚙🔗🗑🔒🗑 |

↑ Add

↓ Add

🗑 Delete

💾 Save

➕ Separator

Finalizando

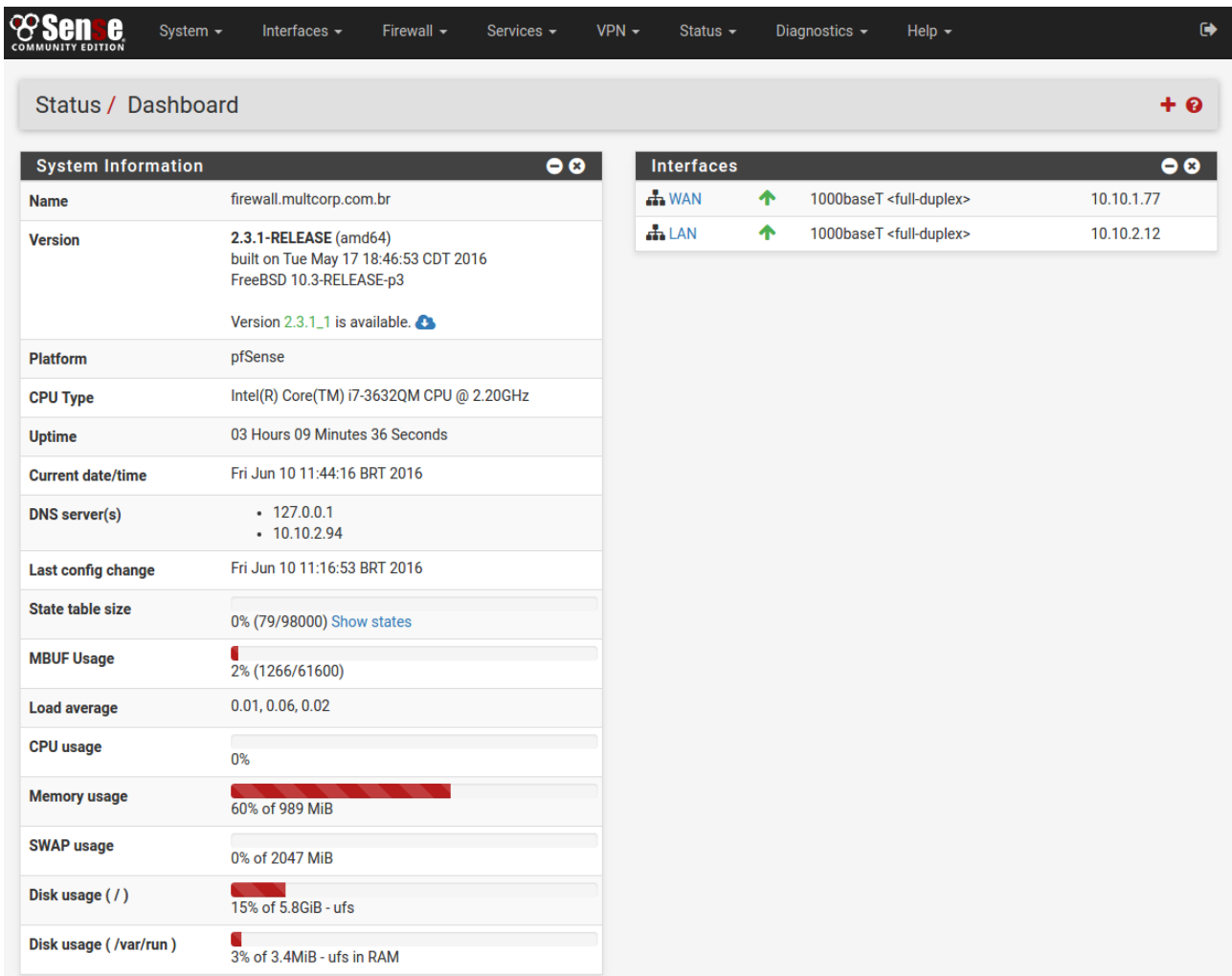
Para finalizar, vamos remover a opção de cliente Gold do menu principal.

Também através do arquivo `/usr/local/www/head.inc`.

Deveremos localizar e remover desse arquivo quatro linhas:

```
$gold_menu = array();  
$gold_menu[] = array(gettext("pfSense Gold"), "https://www.pfsense.org/gold");  
$gold_menu = msort(array_merge($gold_menu, return_ext_menu("Gold")), 0);  
['name' => 'Gold',          'menu' => $gold_menu,          'href' => '_blank'],
```

Após isso podemos atualizar a página e o menu Gold não será mais exibido:



The screenshot displays the pfSense Status / Dashboard page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two panels:

- System Information:** A table showing system details such as Name (firewall.multicorp.com.br), Version (2.3.1-RELEASE), Platform (pfSense), CPU Type (Intel(R) Core(TM) i7-3632QM CPU @ 2.20GHz), Uptime (03 Hours 09 Minutes 36 Seconds), Current date/time (Fri Jun 10 11:44:16 BRT 2016), DNS server(s) (127.0.0.1, 10.10.2.94), Last config change (Fri Jun 10 11:16:53 BRT 2016), State table size (0% (79/98000)), MBUF Usage (2% (1266/61600)), Load average (0.01, 0.06, 0.02), CPU usage (0%), Memory usage (60% of 989 MiB), SWAP usage (0% of 2047 MiB), Disk usage (/) (15% of 5.8GiB - ufs), and Disk usage (/var/run) (3% of 3.4MiB - ufs in RAM).
- Interfaces:** A table showing network interfaces. The WAN interface is configured with 1000baseT <full-duplex> and IP address 10.10.1.77. The LAN interface is configured with 1000baseT <full-duplex> and IP address 10.10.2.12.

Fim dos procedimentos, agora basta ajustar os parâmetros de acordo com a necessidade de cada cliente.

Nesse momento qualquer estação de trabalho da rede configurada para receber IP dinamicamente via DHCP, irá receber um IP da rede LAN, Navegar via proxy automaticamente e com proteção de acessos http e https fora do proxy.

Todos os acessos serão registrados e estarão disponíveis através do relatório.

Fernando Buzon Macedo
fernandobuzon@gmail.com