

**PFSense,
INSTALACIÓN CONFIGURACIÓN Y ADMINISTRACIÓN**

Profesor Pedro Enrique Guerrero Zuluaga

Christian Camilo Gaviria Castro.
Estudiante de Telecomunicaciones
Noviembre 17 de 2016.

Instituto Tecnológico Metropolitano.
Facultad de Ingenierías.
Medellín.

Los servidores son una parte muy importante de una infraestructura de redes ya que estos se encargan de proveer servicios a los clientes tales como almacenamiento de archivos, distribución de algunas aplicaciones, seguridad, alta escalabilidad, centralización de la red, entre otras muchas ventajas, todo esto con el propósito de satisfacer al usuario final. Los servidores deben tener ciertas características físicas para poder cumplir con requisitos de rendimiento y disponibilidad. El software y el hardware de un servidor son generalmente muy determinantes, un hardware regular de un computador personal no puede servir a cierta cantidad de clientes y no podría soportar la escalabilidad por parte de usuarios y demás máquinas debido al alto requerimiento de rendimiento, hay otro factor que influye en esta parte, es la de infraestructura física, de nada sirve tener un servidor con excelentes características si tenemos una infraestructura de red deficiente, lenta e inestable, se debe garantizar una velocidad apta, redundancia en la red y se recomienda al menos cableado de fibra óptica para garantizar una alta velocidad en la transmisión de datos, buen ancho de banda y el ofrecimiento óptimo de los servicios hacia los usuarios finales.

En las próximas páginas de este pequeño anexo se desarrollará la configuración de diferentes servidores para propósitos que se explicarán más adelante.

Tabla de Contenidos

iii

Capítulo 1 Desarrollo de contenidos	1
Significados en Pfsense.....	27
Capítulo 2 Usuarios y contraseñas	32

Capítulo 1

Desarrollo de contenidos

Junto con el profesor Pedro guerrero, asesor de nuestro trabajo de grado y cabeza del semillero de redes, se ha instalado, configurado y administrado una serie de servidores para cubrir las diferentes necesidades de los usuarios y resolver varios problemas que se presentan en las diferentes infraestructuras.

En el laboratorio de radiopropagación ubicado en el sexto piso remotamente accedimos a un servidor ubicado en el departamento de Putumayo para realizar la instalación de un servidor proxy transparente para así mejorar un poco la seguridad de la red, mejorar la velocidad de navegación de los usuarios, mejorar la calidad del servicio en la navegación en internet, disminuir notoriamente el ancho de banda y la latencia y tener una administración centralizada de la misma.

Link de descarga PfSense: <https://pfsense.org/download/>

La configuración fue la siguiente:

```
round-trip min/avg/max/stddev = 19.052/20.149/21.169/0.822 ms
[2.3.2-RELEASE][root@Ingenieros.localdomain]/root: exit
exit
*** Welcome to pfSense 2.3.2-RELEASE (i386 full-install) on Ingenieros ***

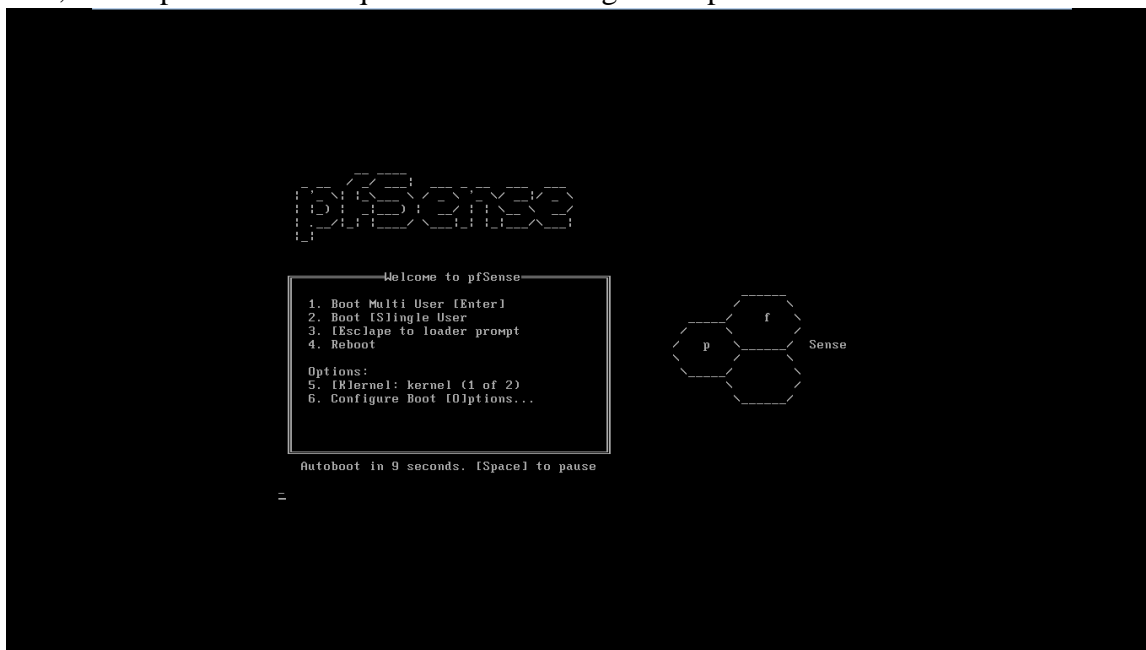
WAN (wan)      -> xn0      -> v4: 192.168.255.2/30
LAN1 (lan)     -> xn1      -> v4: 192.168.100.1/24
GESTION (opt1) -> xn2      -> v4: 192.168.254.11/24
LAN2 (opt2)    -> xn3      -> v4: 172.16.48.1/22
LAN3 (opt3)    -> xn4      -> v4: 172.16.40.1/22
LAN4 (opt4)    -> xn5      -> v4: 172.16.44.1/22
LAN5 (opt5)    -> xn6      -> v4: 192.168.101.1/24

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) PHP shell + pfSense tools
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

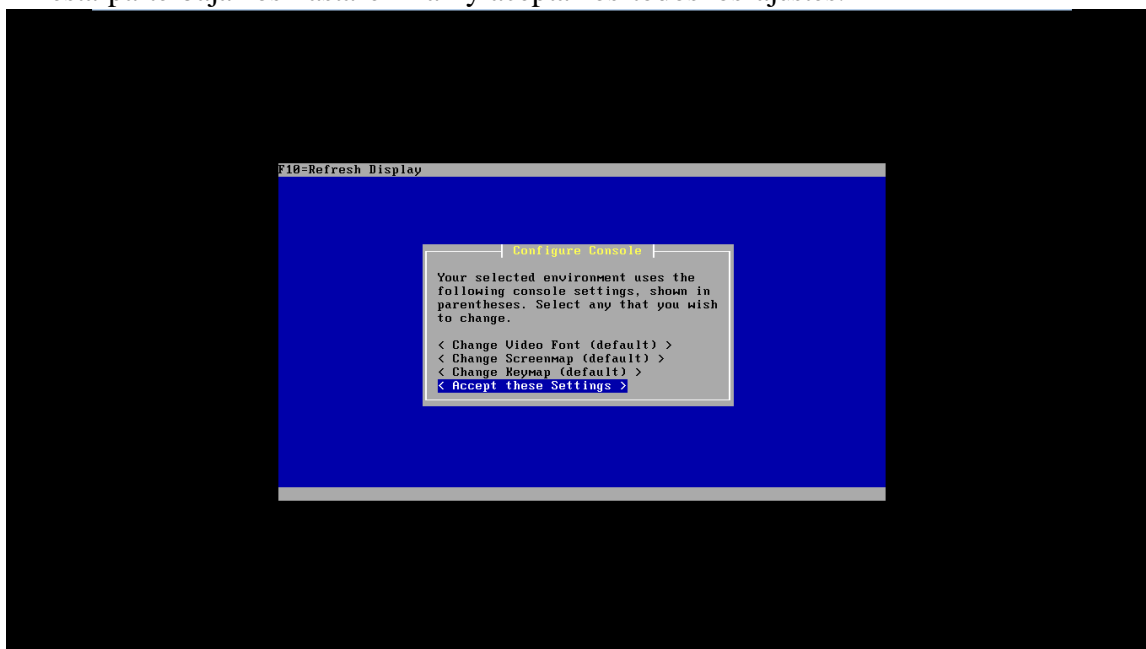
Enter an option: █
```

Para llevar a cabo esto instalamos una máquina virtual en el hipervisor XenServer, el sistema operativo implementado fue PfSense. A continuación se mostrará paso por paso la instalación, configuración y administración.

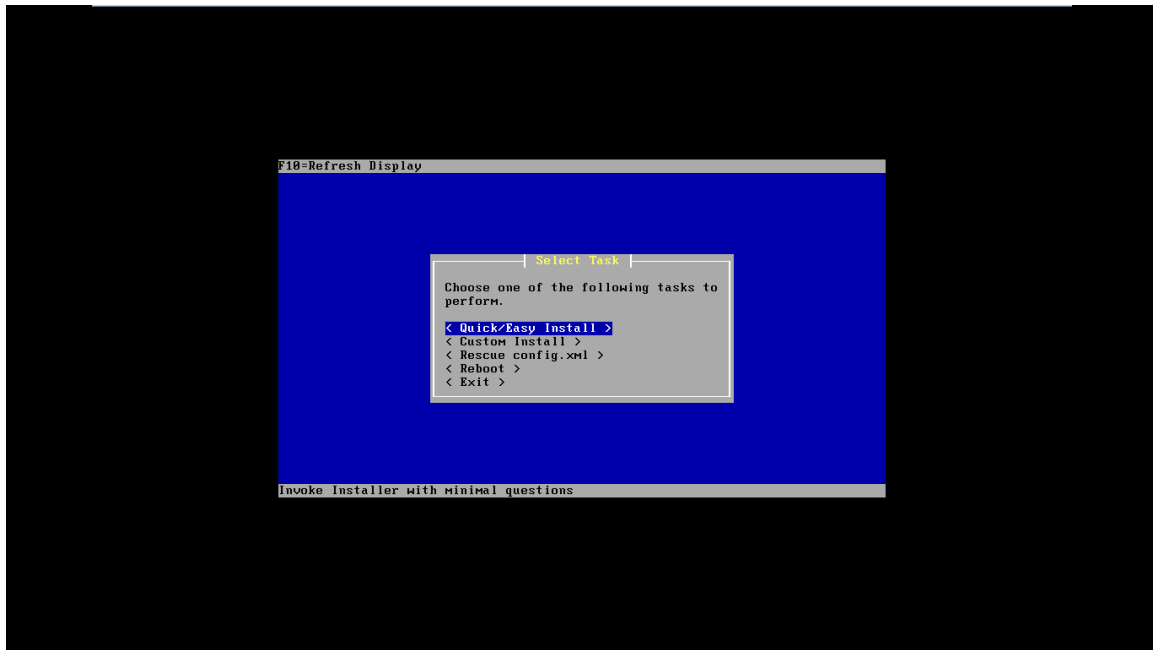
Esta es la pantalla con la que nos encontraremos la primera vez que iniciemos desde el ISO, solo esperamos hasta que entremos a la siguiente pantalla.



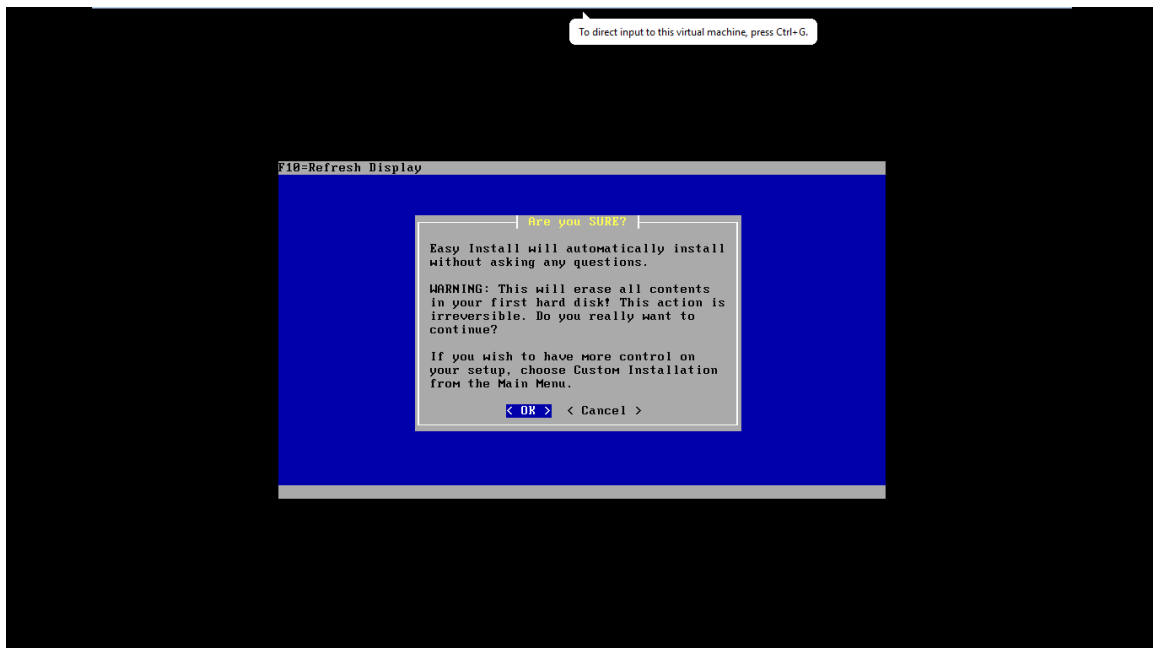
En esta parte bajamos hasta el final y aceptamos todos los ajustes.



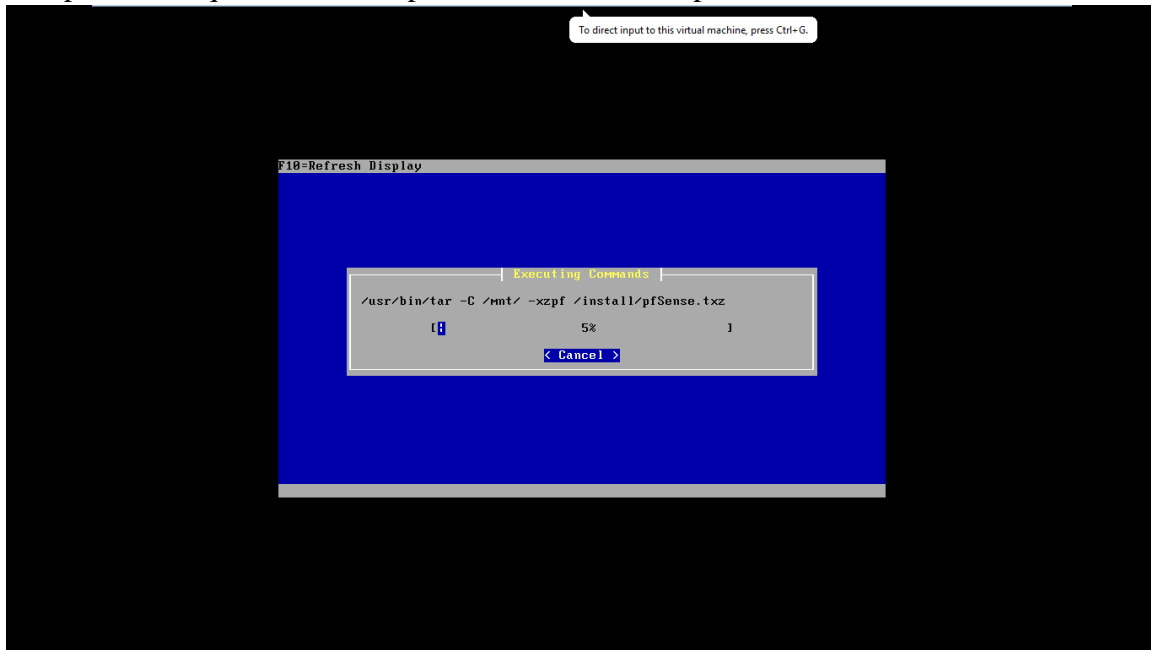
Seleccionamos la instalación fácil.



Confirmamos.



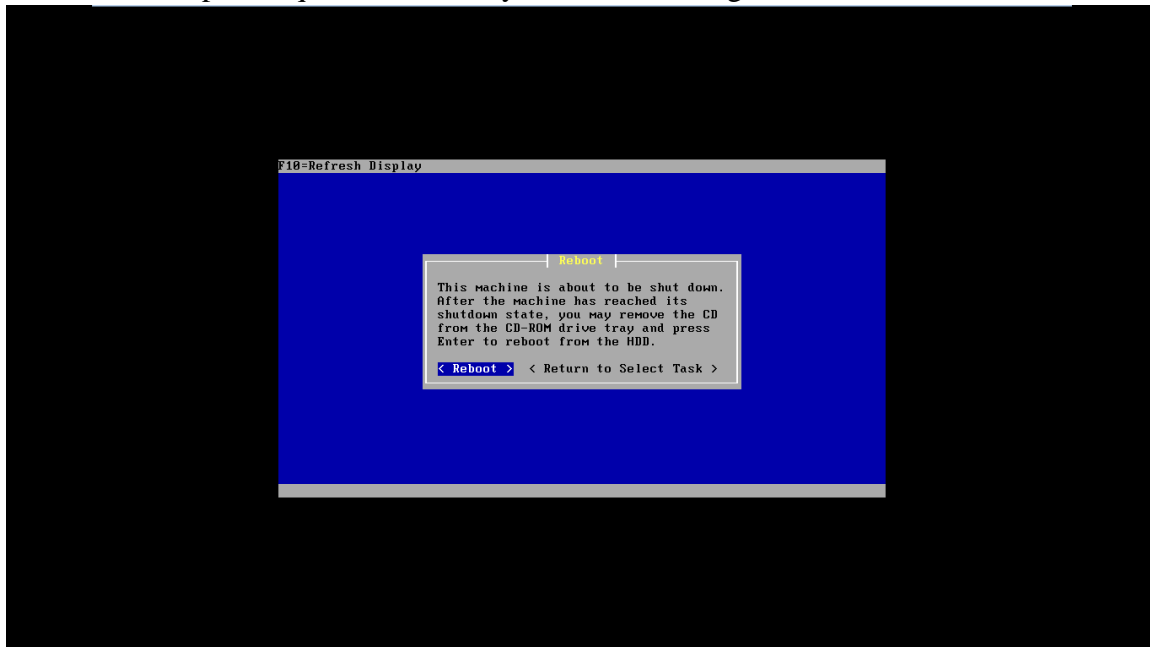
Y esperamos a que el sistema operativo realice las respectivas instalaciones.



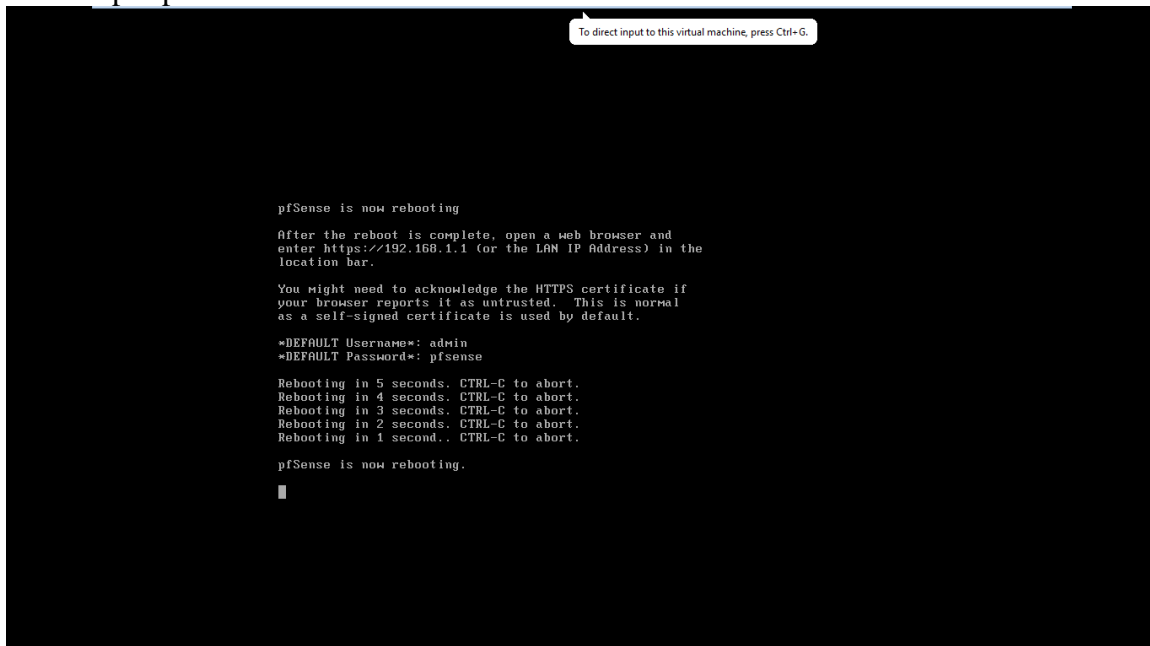
Seleccionamos un kernel estándar y presionamos enter.



Por último nos pedirá que reiniciemos y retiramos la imagen ISO.



En esta pantalla nos muestra como son las credenciales de usuario con las que podemos acceder por primera vez al sistema.



En algunas ocasiones nuestro servidor nos configurará IPs automáticamente, de no ser así se puede configurar seleccionando la opción número 2.

```
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3.2-RELEASE amd64 Tue Jul 19 12:44:43 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.66/24
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) PHP shell + pfSense tools
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
```

Nos mostrará esta opción y podremos configurar nuestras redes como deseemos.
Nota: Por defecto pfsense solo permite acceder a la configuración web solo por su interfaz LAN.

```
To direct input to this virtual machine, press Ctrl-G.

*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.66/24
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) PHP shell + pfSense tools
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 - dhcp, dhcp6)
2 - LAN (em1 - static)

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

Seguiremos los pasos y al final nuestra nueva red quedará lista para que nuestro servidor pfSense pueda ser administrado vía web.

```

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:
> 192.168.10.254

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 LAN, 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

```

Con la dirección que se nos indica accederemos para configurar el servidor por primera vez.

```

DHCPD...

The IPv4 LAN address has been set to 192.168.10.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://192.168.10.254/

Press <ENTER> to continue.
*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***

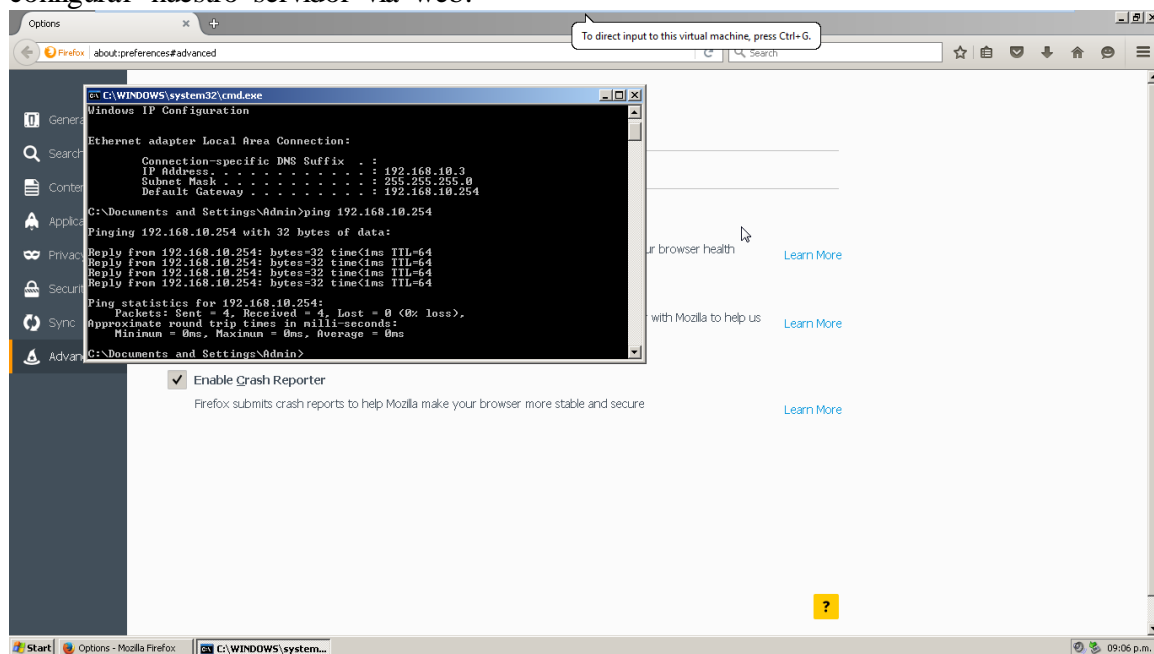
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.66/24
LAN (lan)      -> em1      -> v4: 192.168.10.254/24

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) PHP shell + pfSense tools
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

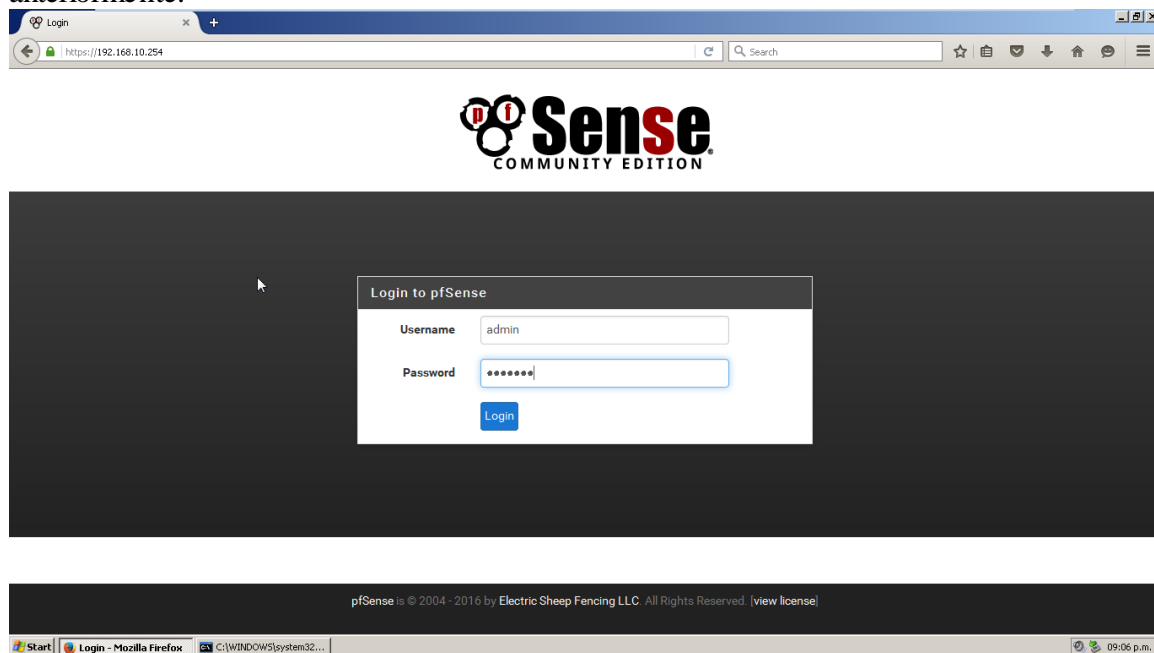
Enter an option: █

```

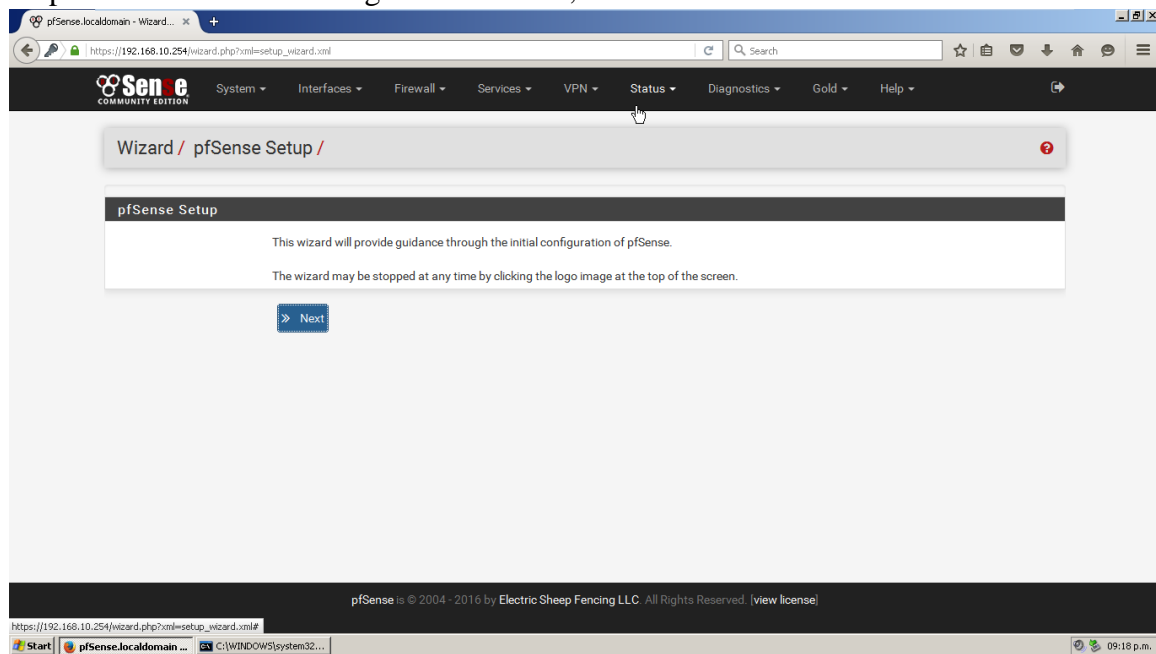
En un PC cliente agregamos una IP en el mismo segmento de red para poder acceder a configurar nuestro servidor vía web.



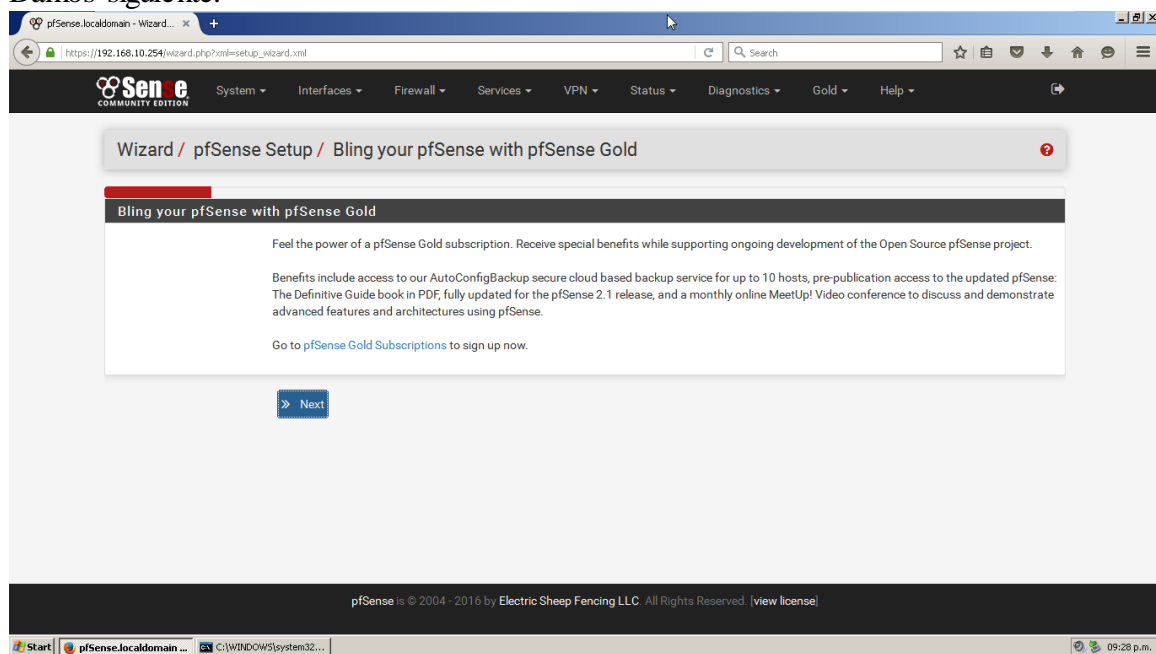
Esta es la página que nos encontraremos, accedemos con las credenciales descritas anteriormente.



Empezaremos con una configuración básica, daremos next.



Damos siguiente.



En este paso pondremos nombre a nuestro servidor, dominio si tenemos, DNS primarios y secundarios y deshabilitamos la opción de que nos entregue DNS por DHCP en la red WAN.

The screenshot shows the 'General Information' step of the pfSense Setup Wizard. The browser address bar shows 'https://192.168.10.254/wizard.php?onl=setup_wizard.xml'. The page title is 'Wizard / pfSense Setup / General Information'. The main heading is 'General Information'. Below it, a message states: 'On this screen the general pfSense parameters will be set.' The form contains the following fields:

- Hostname:** 'Ingenieros' (with a tooltip example: 'myserver').
- Domain:** 'MyDomain' (with a tooltip example: 'mydomain.com').
- Primary DNS Server:** '200.13.249.101'.
- Secondary DNS Server:** '200.13.224.254'.
- Override DNS:** A checkbox labeled 'Allow DNS servers to be overridden by DHCP/PPP on WAN' which is currently unchecked.

A 'Next' button is at the bottom right. The footer shows 'pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]'.

Seleccionamos nuestra zona horaria y el respectivo servidor NTP y continuamos con la configuración.

The screenshot shows the 'Time Server Information' step of the pfSense Setup Wizard. The browser address bar shows 'https://192.168.10.254/wizard.php?onl=setup_wizard.xml'. The page title is 'Wizard / pfSense Setup / Time Server Information'. The main heading is 'Time Server Information'. Below it, a message states: 'Please enter the time, date and time zone.' The form contains the following fields:

- Time server hostname:** '0.south-america.pool.ntp.org' (with a tooltip example: 'Enter the hostname (FQDN) of the time server.').
- Timezone:** A dropdown menu showing 'America/Bogota'.

A 'Next' button is at the bottom right. The footer shows 'pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]'.

En esta parte configuraremos nuestra red WAN, en este caso la configuraremos con IP estática y damos en siguiente.

Wizard / pfSense Setup / Configure WAN Interface

Configure WAN Interface

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

SelectedType Static

General configuration

MAC Address

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: xxxxxxxxxx or leave blank.

MTU

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.

MSS

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.

Static IP Configuration

IP Address 192.168.1.200

Subnet Mask 24

Upstream Gateway 192.168.1.254

DHCP client configuration

DHCP Hostname

The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

PPPoE configuration

PPPoE Username

PPPoE Password

Show PPPoE password ☐ Reveal password characters

PPPoE Service name

Hint: this field can usually be left empty

PPPoE Dial on demand ☐ Enable Dial-On-Demand mode

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.

On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

DHCPv6 Client Configuration	
Options	<input type="checkbox"/> Advanced Configuration Use advanced DHCPv6 configuration options. <input type="checkbox"/> Configuration Override Override the configuration from this file.
Use IPv4 connectivity as parent interface	<input type="checkbox"/> Request a IPv6 prefix/information through the IPv4 connectivity link
Request only an IPv6 prefix	<input type="checkbox"/> Only request an IPv6 prefix, do not request an IPv6 address
DHCPv6 Prefix Delegation size	<input type="text" value="64"/> The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the ISP.
Send IPv6 prefix hint	<input type="checkbox"/> Send an IPv6 prefix hint to indicate the desired prefix size for delegation
Debug	<input type="checkbox"/> Start DHCPv6 client in debug mode
Reserved Networks	
Block private networks and loopback addresses	<input type="checkbox"/> Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input type="checkbox"/> Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

[Save](#)

pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license](#)

Configuramos nuestra red LAN y continuamos.

pfSense.localdomain - Wizard... +

https://192.168.10.254/wizard.php?xml=setup_wizard.xml

To direct input to this virtual machine, press Ctrl+G.

Sen e COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Gold ▾ Help ▾

Wizard / pfSense Setup / Configure LAN Interface ?

Configure LAN Interface	
On this screen the Local Area Network information will be configured.	
LAN IP Address	<input type="text" value="192.168.10.254"/> Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask	<input type="text" value="24"/>

[Next](#)

pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license](#)

Start | pfSense.localdomain... | C:\WINDOWS\system32... | 09:57 p.m.

Las demás interfaces de red locales se configuran de manera similar.

MTU

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

MSS

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.

Speed and Duplex

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

IPv4 Upstream gateway [Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses ☐ Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks ☐ Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

[Save](#)

pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license](#)

En esta parte configuramos la contraseña a nuestro gusto.

pfSense.localdomain - Wizard... [To direct input to this virtual machine, press Ctrl+G.](#)

https://192.168.10.254/wizard.php?xml=setup_wizard.xml

Sen e COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Wizard / pfSense Setup / Set Admin WebGUI Password

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

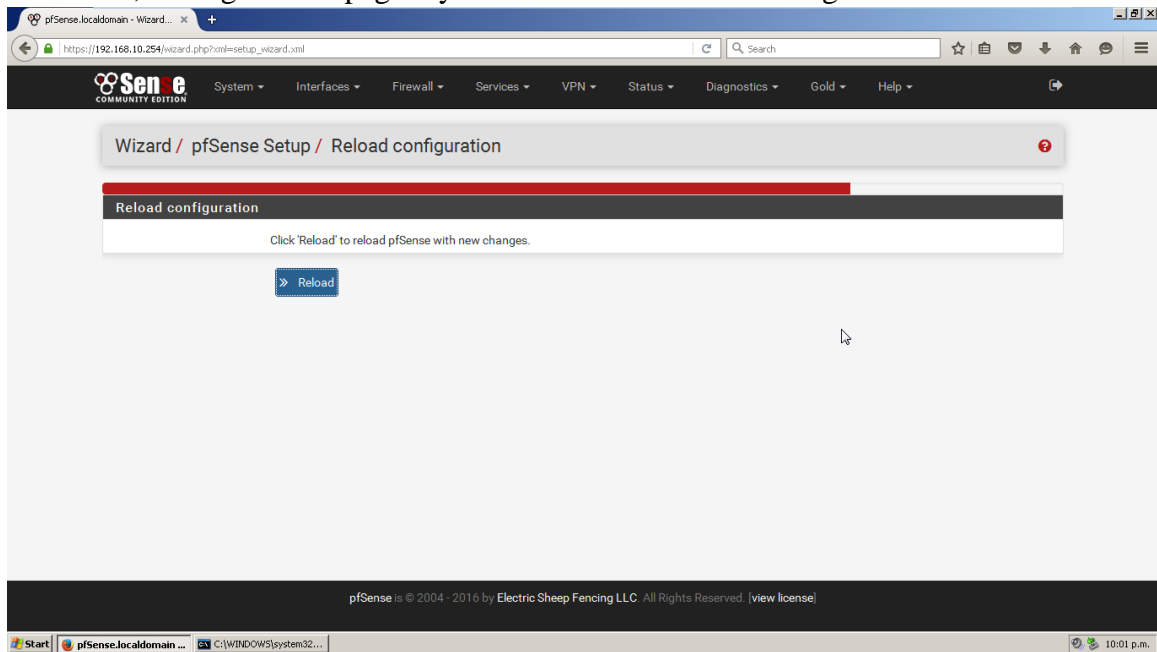
Admin Password AGAIN

[Next](#)

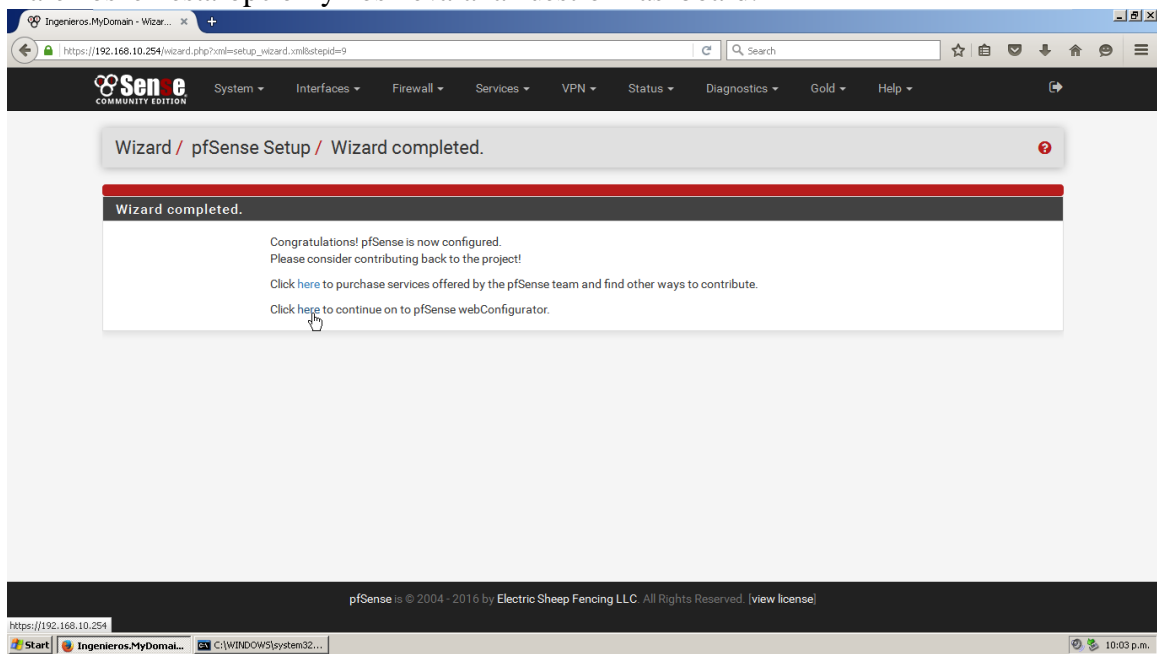
pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license](#)

Start pfSense.localdomain... C:\WINDOWS\system32... 09:58 p.m.

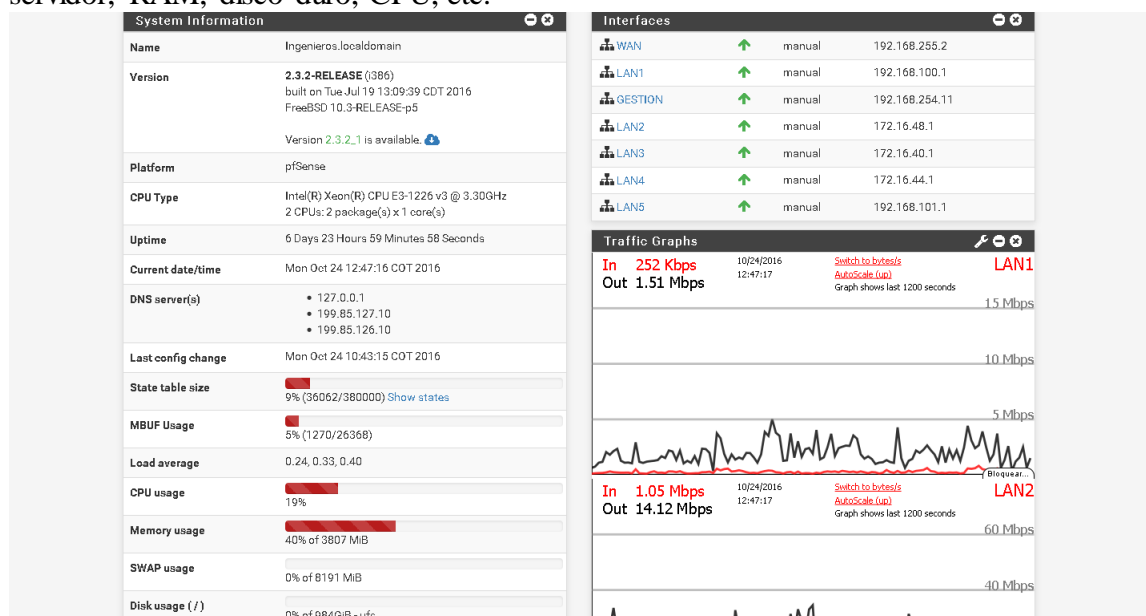
Por último, recargamos la página y estará casi lista nuestra configuración básica.



Daremos en esta opción y nos llevara a nuestro Dashboard.

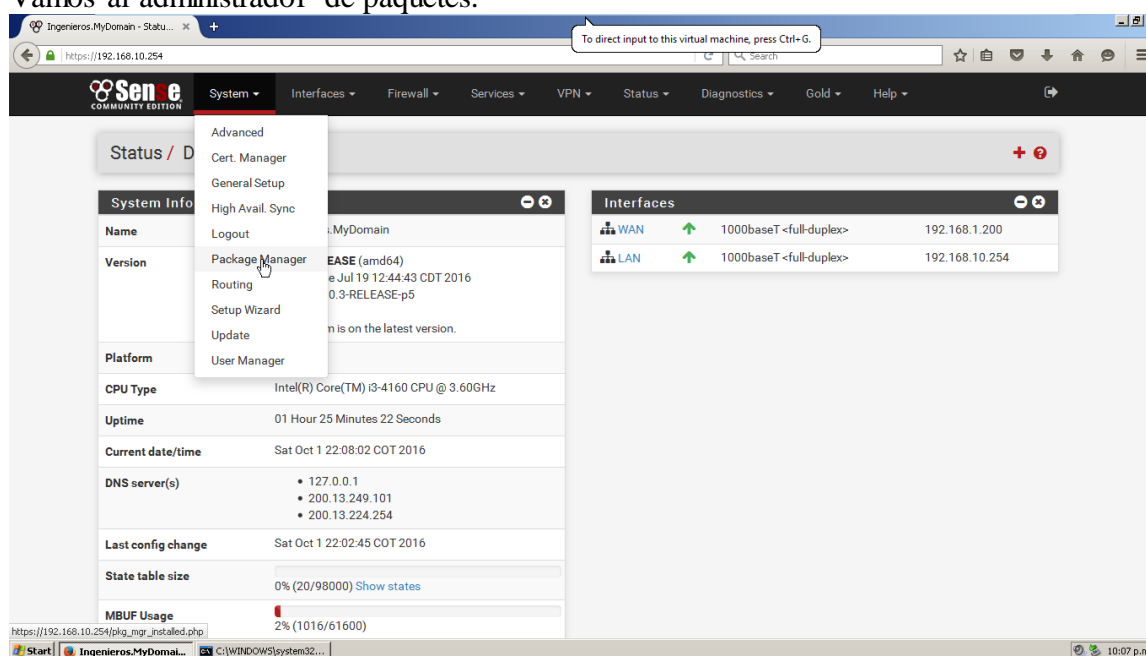


Este es nuestro Dashboard, desde aquí podemos monitorear lo que sucede con nuestro servidor, RAM, disco duro, CPU, etc.



A partir de este momento instalaremos y configuraremos nuestro servidor como proxy transparente:

Vamos al administrador de paquetes.



Vamos a paquetes disponibles, buscamos el paquete Squid y lo instalamos.

The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "System / Package Manager / Available Packages".

Under the "Available Packages" tab, there is a search bar and a table of available packages:

Name	Version	Description	Action
apcupsd	0.3.9_1	"apcupsd" can be used for controlling all APC UPS models. It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN. Package Dependencies: apcupsd-3.14.13	+ Install
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.	+ Install

Below the table, a green banner indicates "Installation successfully completed." The "Package Installer" tab is selected, showing the installation details for Squid:

```

===> NOTICE:

The c-icap-modules port currently does not have a maintainer. As a result, it is
more likely to have unresolved issues, not be up-to-date, or even be removed in
the future. To volunteer to maintain this port, please create an issue at:

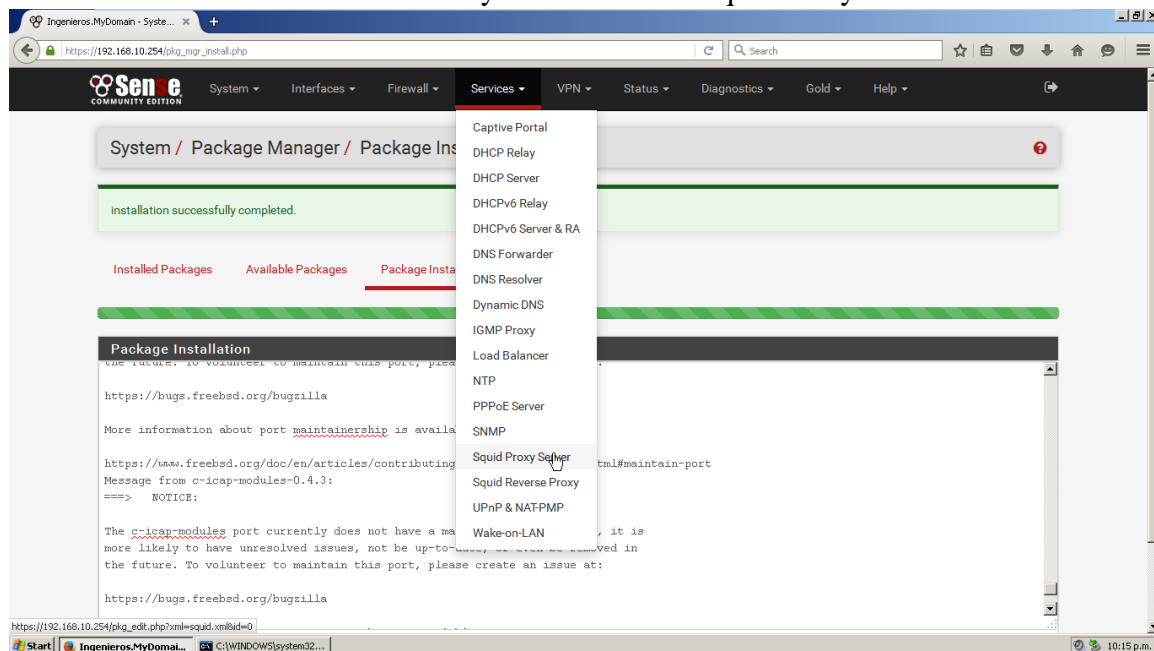
https://bugs.freebsd.org/bugzilla

More information about port maintainership is available at:

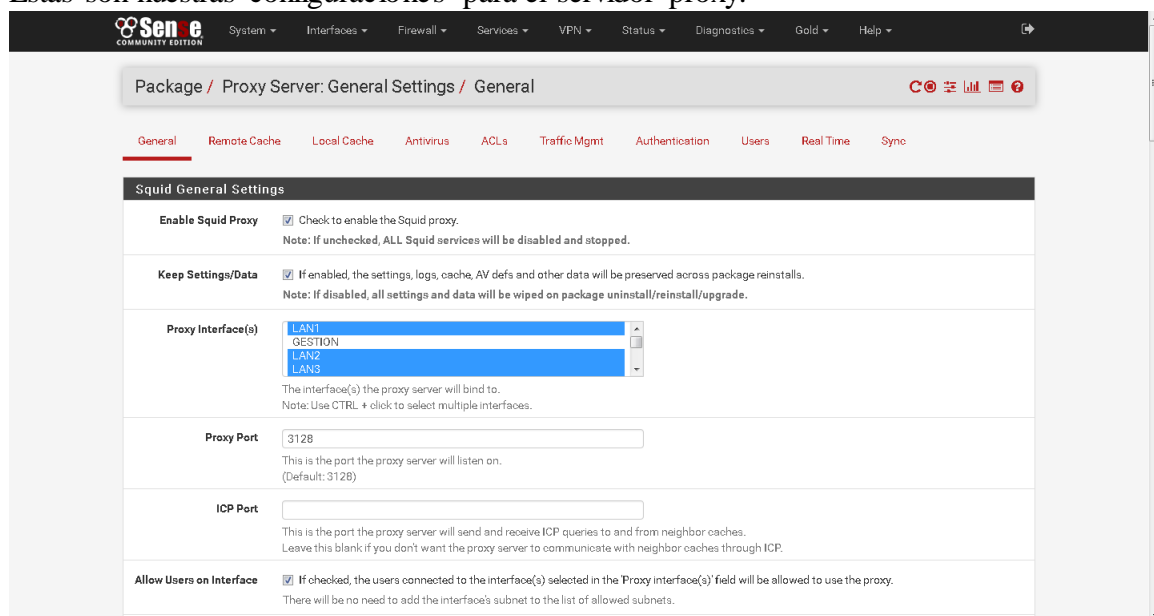
https://www.freebsd.org/doc/en/articles/contributing/ports-contributing.html#maintain-port
Message from pfSense-pkg-squid-0.4.23:
Please visit Services - Squid Proxy Server menu to configure the package and enable the proxy.
>>> Cleaning up cache... done.
Success
  
```

The footer of the interface shows "pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]"

Una vez instalado vamos a servicios y seleccionamos Squid Proxy Server.



Estas son nuestras configuraciones para el servidor proxy.



Haremos las siguientes configuraciones para establecer nuestro servidor como proxy transparente:


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 same copy of the file from pfSense GitHub repository if needed.
Resolve DNS IPv4 First	<input checked="" type="checkbox"/> Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.
Disable ICMP	<input type="checkbox"/> Check this to disable Squid ICMP pinger helper.
Use Alternate DNS Servers for the Proxy Server	<input type="text" value="8.8.8.8"/> If you want to use DNS servers other than the DNS forwarder/resolver configured in pfSense, enter the IP(s) here. Note: Separate entries by semi-colons (;)
Transparent Proxy Settings	
Transparent HTTP Proxy	<input checked="" type="checkbox"/> Enable transparent mode to forward all requests for destination port 80 to the proxy server without any additional configuration being necessary. Note: Transparent mode will filter SSL (port 443) if you enable man-in-the-middle options below. In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections, configure WPAD/PAC options on your DNS/DHCP servers.
Transparent Proxy Interface(s)	<div><input type="text" value="LAN1"/> <input type="text" value="GUESTION"/> <input type="text" value="LAN2"/> <input type="text" value="LAN3"/></div> The interface(s) the proxy server will transparently intercept requests on. Note: Use CTRL + click to select multiple interfaces.
Bypass Proxy for Private Address Destination	<input type="checkbox"/> Do not forward traffic to Private Address Space (RFC 1918) destinations. Destinations in Private Address Space (RFC 1918) are passed directly through the firewall, not through the proxy server.
Bypass Proxy for These Source IPs	<input type="text"/> Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. (Applies only to transparent mode.) Note: Separate entries by semi-colons (;)
Bypass Proxy for These Source IPs	<input type="text"/> Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. (Applies only to transparent mode.) Note: Separate entries by semi-colons (;)
Bypass Proxy for These Destination IPs	<input type="text"/> Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. (Applies only to transparent mode.) Note: Separate entries by semi-colons (;)
SSL Man in the Middle Filtering	
HTTPS/SSL Interception	<input type="checkbox"/> Enable SSL filtering.
SSL Intercept Interface(s)	<div><input type="text" value="LAN1"/> <input type="text" value="GUESTION"/> <input type="text" value="LAN2"/> <input type="text" value="LAN3"/></div> The interface(s) the proxy server will intercept SSL requests on. Note: Use CTRL + click to select multiple interfaces.
SSL Proxy port	<input type="text"/> This is the port the proxy server will listen on to intercept SSL while using transparent proxy. (Default: 3129)
CA	<div><input type="text" value="none"/></div> Select Certificate Authority to use when SSL interception is enabled. To create a CA on pfSense, go to System -> Cert Manager . Install the CA certificate as a Trusted Root CA on each computer you want to filter SSL on to avoid SSL error on each connection.
SSL Certificate Daemon Children	<input type="text"/> This is the number of SSL certificate daemon children to start. If Squid is used in busy environments, this may need to be increased. Default: 5
Remote Cert Checks	<div><input type="text" value="Accept remote server certificate with errors"/> <input type="text" value="Do not verify remote certificates"/></div>

Remote Cert Checks	<input type="text" value="Accept remote server certificate with errors"/> <input type="text" value="Do not verify remote certificate"/>
Select remote SSL certificate checks to perform. Note: Use CTRL + click to select multiple options.	
Certificate Adapt	<input type="text" value="Sets the 'Not After' (setValidAfter)"/> <input type="text" value="Sets the 'Not Before' (setValidBefore)"/> <input type="text" value="Sets CN property (setCommonName)"/>
Pass original SSL server certificate information to the user. Allow the user to make an informed decision on whether to trust the server certificate. Hint: Set the subject CN - see fake certificate properties documentation for details.	
Logging Settings	
Enable Access Logging	<input checked="" type="checkbox"/> This will enable the access log. Warning: Do not enable if disk capacity is low.
Log Store Directory	<input type="text" value="/var/squid/logs"/> The directory where the logs will be stored. This is also used for logs other than the Access Log above. Default: /var/squid/logs Note: Do NOT include the trailing / when setting a custom location.
Rotate Logs	<input type="text" value="8"/> Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
Log Pages Denied by SquidGuard	<input type="checkbox"/> Makes it possible for SquidGuard denied log to be included on Squid logs. Note: This option will only work if you include the code below in your sgerror.php file. This forces the client browser to send a second request to Squid with the denied string in URL. <pre>\$sge_prefix = (preg_match("/\?/", \$ol[u]) ? "&": "?"); \$str[] = "<iframe> src=\"\$sge_prefix . \$gr=ACCESSDENIED\" width=\"1\" height=\"1\"></iframe>";</pre> Hint: You MUST remove extra spaces in the above iframe HTML tags.

Finalizamos guardando nuestra configuración.

Headers Handling, Language and Other Customizations	
Visible Hostname	<input type="text" value="Ingenieros"/> This is the hostname to be displayed in proxy server error messages.
Administrator's Email	<input type="text" value="soportemillennium@gmail.com"/> This is the email address displayed in error messages to the users.
Error Language	<input type="text" value="en"/> Select the language in which the proxy server will display error messages to users.
X-Forwarded Header Mode	<input type="text" value="transparent"/> on: Squid will append your client's IP address in the HTTP requests it forwards. The header looks like: X-Forwarded-For: 192.1.2.3. off: Squid will NOT append your client's IP address in the HTTP requests it forwards. The header looks like: X-Forwarded-For: unknown transparent: Squid will not alter the X-Forwarded-For header in any way. delete: Squid will delete the entire X-Forwarded-For header. truncate: Squid will remove all existing X-Forwarded-For header entries and place the client's IP address as the only header entry. Default: on
Disable VIA Header	<input type="checkbox"/> If not set, Squid will include a Via header in requests and replies as required by RFC2616.
URI Whitespace Characters Handling	<input type="text" value="strip"/> strip: The whitespace characters are stripped out of the URI. This is the behavior recommended by RFC2396. deny: The request is denied. The user receives an "Invalid Request" message. allow: The request is allowed and the URI is not changed. The whitespace characters remain in the URI. encode: The request is allowed and the whitespace characters are encoded according to RFC1738. chop: The request is allowed and the URI is chopped at the first whitespace.
Suppress Squid Version	<input checked="" type="checkbox"/> Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.
<input type="button" value="Save"/> <input type="button" value="Show Advanced Options"/>	
pfsense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. view license	

Ahora nos dirigimos a la pestaña de local cache.


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

Package / Proxy Server: Cache Management / Local Cache

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

Squid Cache General Settings

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.

Heap LFUDA: Keeps popular objects in cache regardless of their size and thus optimizes byte hit rate at the expense of hit rate.
Heap GDSF: Optimizes object-hit rate by keeping smaller, popular objects in cache.
Heap LRU: Works like LRU, but uses a heap instead.
LRU: Keeps recently referenced objects (i.e., replaces the object that has not been accessed for the longest time).
Please see [cache_replacement_policy documentation](#) for additional details.

Default: heap LFUDA

Low-Water Mark in %

90

The low-water mark for ADFS/DFS/diskd cache object eviction by the cache_replacement_policy algorithm.
Cache replacement begins when the swap usage is above this low-water mark and attempts to maintain utilisation near the low-water mark.
Please see [cache_swap_low documentation](#) for additional details.

High-Water Mark in %

95

The high-water mark for ADFS/DFS/diskd cache object eviction by the cache_replacement_policy algorithm.
As swap utilization increases towards this high-water mark, object eviction becomes more aggressive.
Please see [cache_swap_high documentation](#) for additional details.

Do Not Cache

Squid Hard Disk Cache Settings

Hard Disk Cache Size

1000000

Amount of disk space (in megabytes) to use for cached objects.

Hard Disk Cache System

ufs ▾

This specifies the kind of storage system to use.

ufs - 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.
null - does not use any storage. Ideal for Embedded/NanoBSD.

Please see [cache_dir documentation](#) for additional details.

Clear Disk Cache NOW

Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron.
The script will only clear the disk cache on the following conditions:
- if the swap.state file is taking up more than 75% of disk space;
- or the drive is 90% full and swap.state is larger than 1GB.

If you wish to clear cache **immediately**, press the Clear Disk Cache NOW button.

Level 1 Directories

16 ▾

Each level-1 directory contains 256 subdirectories, so a value of 256 level-1 directories will use a total of 65536 directories for the hard disk cache.
This will **significantly** slow down the startup process of the proxy service, but can speed up the caching under certain conditions.

Hard Disk Cache Location

/var/squid/cache

This is the directory where the cache will be stored. If you change this location, Squid needs to make a new cache, this could take a while.
Default: /var/squid/cache
Note: Do NOT include the trailing / when setting a custom location.

Minimum Object Size

0

Objects smaller than the size specified (in kilobytes) will not be saved on disk.
Default: 0 (meaning there is no minimum)

Minimum Object Size	<input type="text" value="0"/>
Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)	
Maximum Object Size	<input type="text" value="50"/>
Objects larger than the size specified (in megabytes) will not be saved on disk. Hint: If increased speed is more important than saving bandwidth, this should be set to a low value. Default: 4 (MB)	
Squid Memory Cache Settings	
Memory Cache Size	<input type="text" value="2048"/>
Specifies the ideal amount of physical RAM (in megabytes) to be used for In-Transit objects, Hot Objects and Negative-Cached objects. Please see cache_mem documentation for additional details. This value should not exceed 50% of the installed RAM. The minimum value is 1MB. Default: 64 (MB)	
Maximum Object Size in RAM	<input type="text" value="512"/>
Objects greater than this size (in kilobytes) will not be attempted to kept in the memory cache. Default: 256 (KB)	
Memory Replacement Policy	<input type="text" value="Heap GDSF"/>
The memory replacement policy determines which objects are purged from memory when space is needed. Heap GDSF: Optimizes object-hit rate by keeping smaller, popular objects in cache. Heap LFUDA: Keeps popular objects in cache regardless of their size and thus optimizes byte hit rate at the expense of hit rate. Heap LRU: Works like LRU, but uses a heap instead. LRU: Keeps recently referenced objects (i.e., replaces the object that has not been accessed for the longest time). Please see cache_replacement_policy documentation for additional details. Default: heap GDSF	
Dynamic and Update Content	
Cache Dynamic Content	<input type="checkbox"/> Select to enable caching of dynamic content

Por último, salvamos la configuración.

Memory Replacement Policy	<input type="text" value="Heap GDSF"/>
The memory replacement policy determines which objects are purged from memory when space is needed. Heap GDSF: Optimizes object-hit rate by keeping smaller, popular objects in cache. Heap LFUDA: Keeps popular objects in cache regardless of their size and thus optimizes byte hit rate at the expense of hit rate. Heap LRU: Works like LRU, but uses a heap instead. LRU: Keeps recently referenced objects (i.e., replaces the object that has not been accessed for the longest time). Please see cache_replacement_policy documentation for additional details. Default: heap GDSF	
Dynamic and Update Content	
Cache Dynamic Content	<input checked="" type="checkbox"/> Select to enable caching of dynamic content. With dynamic cache enabled, you can also apply refresh_patterns to sites like Windows Updates Notes: - Squid wiki suggests setting 'Finish transfer if less than xKB remaining' on 'Traffic Mgmt' tab to -1 (but you can apply your own values to control cache). - Set 'Maximum Download Size' on 'Traffic Mgmt' tab to a value that fits patterns you are applying.
Custom refresh_patterns	<div><input type="text"/></div> Enter custom refresh_patterns for better dynamic cache usage. Note: These refresh_patterns will only be included if 'Cache Dynamic Content' is enabled.
<div> Save</div>	



Ahora configuraremos un antivirus para nuestro servidor proxy.

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.

Y guardamos la configuración.

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 every 24 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**

pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [\[view license\]](#)

Vamos a la pestaña de ACLs y permitimos las subredes en donde aplicaremos nuestro proxy transparente.

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 [192.168.100.0/24
172.16.48.0/22
172.16.40.0/22
172.16.44.0/22
192.168.101.0/24]

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.

Unrestricted IPs

Enter unrestricted IP address(es) / network(s) in CIDR format.
Configured entries will NOT be filtered out by the other access control directives set in this page.
Note: Put each entry on a separate line.

Banned Hosts Addresses

Agregamos los puertos básicos que se permitirán en el servidor y salvamos los cambios.

Destination domains that will be blocked for the users that are allowed to use the proxy.
Note: Put each entry on a separate line. You also can use regular expressions.

Block User Agents

Enter user agents that will be blocked for the users that are allowed to use the proxy.
Note: Put each entry on a separate line. You also can use regular expressions.

Block MIME Types (Reply Only)

Enter MIME types that will be blocked for the users that are allowed to use the proxy. Useful to block javascript (application/javascript).
Note: Put each entry on a separate line. You also can use regular expressions.

Squid Allowed Ports

ACL SafePorts 80 443
This is a space-separated list of 'safe ports' in addition to the predefined default list.
Default list: 21 70 80 210 280 443 488 563 591 631 777 901 1025-65535

ACL SSLPorts 443
This is a space-separated list of ports to allow SSL "CONNECT" to in addition to the predefined default list.
Default list: 443 563

Save

pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

Con esta configuración los usuarios ya deberían poder navegar en internet, para verificar esto nos iremos a la pestaña “Real time”, desde acá podemos administrar y observar a qué tipo de páginas están accediendo los diferentes usuarios

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

Filtering

Max lines: 15 lines
Max. lines to be displayed.

String filter:

Enter a grep-like string/pattern to filter the log entries.
E.g.: username, IP address, URL.
Use ! to invert the sense of matching (to select non-matching lines).

Squid Access Table

Date	IP	Status	Address	UserDestination
24.10.2016 12:43:47	172.16.40.40	TCP_MISS/200	http://dl.delivery.mp.microsoft.com/filestreamingservice/files/e9d78bac-8bdd-455b-891b-32dde6065d73	- 13.107.4.50
24.10.2016 12:43:47	172.16.40.76	TCP_MISS/200	http://alog.umeng.com/app_logs	- 110.173.196.36
24.10.2016 12:43:47	172.16.40.232	TCP_MISS/200	http://cdn.sniper3d.fungames-forfree.com/bundles/android/908/WeaponPartRPG7MissileStore	- 54.230.163.168
24.10.2016 12:43:47	172.16.50.206	TCP_MISS/206	http://r6--sn-cv67ln7e.googlevideo.com/videoplayback?	- 173.194.136.172
24.10.2016 12:43:47	172.16.51.205	TCP_MISS/301	http://g.oepmnsn.com/BSE/413?	- 65.55.2.82
24.10.2016 12:43:47	172.16.40.146	TCP_MISS/200	http://d.billyfcontent.com/gw?	- 62.212.87.141
24.10.2016 12:43:47	192.168.101.214	TCP_MISS/200	http://igcdn-photos-h-a.akamaihd.net/hphotos-ak-xpa1/t51.2885-15/s150x150/e35/13531962_657246394428223_855013838_n.jpg	- 23.73.180.41
24.10.2016 12:43:47	172.16.40.25	TCP_MEM_HIT/200	http://www.bbm.com/appinfo/ver/Android.json	-
24.10.2016 12:43:47	172.16.40.146	TCP_MISS/302	http://d.billyfcontent.com/d/4993560285e36828?	- 62.212.87.141
24.10.2016 12:43:47	172.16.40.218	TCP_MISS/200	http://oe-global-track-prod-1119723899.ap-northeast-1.elb.amazonaws.com/api/1/tracking	- 54.250.232.230
24.10.2016 12:43:47	172.16.40.81	TCP_MISS/200	http://ads.mopub.com/m/ad?	- 192.44.68.4
24.10.2016 12:43:47	172.16.40.5	TCP_MISS/200	http://my.mobfox.com/request.php?	- 184.172.192.51
24.10.2016 12:43:47	172.16.40.5	TCP_MISS/200	http://my.mobfox.com/request.php?	- 184.172.192.50
24.10.2016 12:43:47	172.16.40.196	TCP_MISS/503	http://inputcloudapi.funnytap.com/inputcloudapi/lang/s/LangSupport?	- 52.74.134.214
24.10.2016 12:43:47	192.168.101.214	TCP_MISS/200	http://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xpa1/t51.2885-15/s150x150/e35/13534425_551793501660238_572862273_n.jpg	- 23.73.180.27

Squid Cache Table

Se recomienda reiniciar el servicio squid una vez finalizada la configuración.

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

Keep Settings/Data ☒ 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) LAN1 LAN2 LAN3
The interface(s) the proxy server will bind to.
Note: Use CTRL + click to select multiple interfaces.

Proxy Port 3128
This is the port the proxy server will listen on.
(Default: 3128)

ICP Port
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 ☒ 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.

Ahora nos dirigiremos a la opción ‘Traffic Graph’

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

Keep Settings/Data ☒ 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) LAN1 LAN2 LAN3
The interface(s) the proxy server will bind to.
Note: Use CTRL + click to select multiple interfaces.

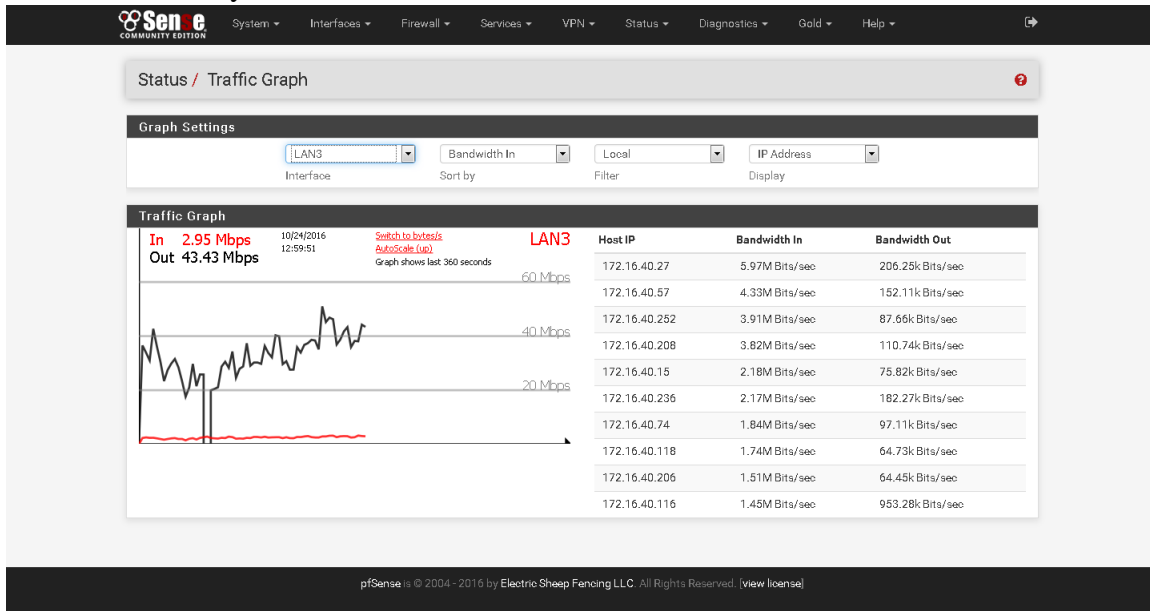
Proxy Port 3128
This is the port the proxy server will listen on.
(Default: 3128)

ICP Port
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 ☒ 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.

Left sidebar menu items: Captive Portal, CARP (failover), Dashboard, DHCP Leases, DHCPv6 Leases, Filter Reload, Gateways, Interfaces, IPsec, Load Balancer, Monitoring, Notes, NTP, OpenVPN, Package Logs, Queues, Services, Squid Proxy Reports, System Logs, Traffic Graph, UPnP & NAT-PMP.

En esta sección nos encontraremos con tablas en donde podemos analizar los diferentes usuarios que están accediendo por las diferentes redes, además de analizar anchos de banda de entrada y salida.



Ahora nos iremos para el apartado de Firewall, en donde observaremos las reglas básicas para permitir tráfico y navegación en las diferentes redes, para hacer esto iremos a Firewall y luego Rules.

Firewall / Rules / LAN3

Floating WAN LAN1 GESTION LAN2 LAN3 LAN4 LAN5

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/90 KIB	IPv4 ICMP	*	*	*	*	*	none			Anchor Edit Delete
✓ 10/-88850441 B	IPv4 *	*	*	*	*	*	none			Anchor Edit Delete
✓ 0/17 KIB	IPv6 *	*	*	*	*	*	none			Anchor Edit Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

Significados en Pfsense

Se destacan en el proxy transparente pfsense las opciones más importantes, su respectiva traducción y explicación, las demás opciones no se destacan ya que son opciones por defecto:

- **Enable Squid Proxy:** Marcar para habilitar el squid proxy, si no se marca, todos los servicios de squid estarán deshabilitados y detenidos.
- **Keep Settings/Data:** Si se marca, los ajustes, registros, caché, antivirus y otros datos serán preservados a través de la reinstalación de paquetes, si está desactivada, todos los ajustes y los datos serán eliminados en el paquete de desinstalación / reinstalación / actualización.
- **ICP Port:** Este es el puerto del servidor proxy enviará y recibirá las consultas ICP hacia y desde cachés vecinas, dejar en blanco si no desea que el servidor proxy se comunique con cachés vecinas mediante ICP.
- **Allow Users on Interface:** Si se selecciona, los usuarios conectados a la interfaz seleccionada en el campo de "Proxy interface(s)" se permitirán para usar el proxy, no habrá necesidad de añadir la subred de interfaces a la lista de subredes permitidas.
- **Resolve DNS IPv4 First:** habilitar esto para forzar la búsqueda de DNS IPv4 primero, esta opción es muy útil si tienes problemas accediendo a sitios HTTPS.
- **Disable ICMP:** Activar esto para desactivar la ayuda de ping ICMP squid.

- **Bypass Proxy for Private Address Destination:** No reenviar el tráfico a destino de espacio a direcciones privadas (RFC 1918), destinos en espacio de direcciones privadas son pasadas directamente a través del firewall, no a través del servidor proxy.
- **Enable Access Logging:** Esto permitirá el acceso al registro, advertencia: no activar si la capacidad del disco es baja.
- **Rotate Logs:** define cuantos días de los archivos de registro se mantendrán. La rotación se desactiva si se deja vacío.
- **Error Language:** Seleccione el idioma en el que el servidor proxy mostrará los mensajes de error a los usuarios.
- **X-Forwarded Header Mode:**

On: Squid anexará la dirección IP en la solicitud reenviar HTTP. El encabezado parece: X-Forwarded-For: 192.1.2.3.

Off: Squid no anexará la dirección IP del cliente en la solicitud reenviar HTTP. El encabezado parece: X-Forwarded-For: unknown

Transparent: Squid no alterará el encabezado de ninguna manera.

Delete: Squid eliminará todo el encabezado.

Truncate: Squid eliminará todas las entradas de encabezado existentes X-Forwarded-For y coloca la dirección IP como la única entrada de encabezado.
- **URI Whitespace Characters Handling:** Identificador uniforme de recursos (URI), es una cadena corta de caracteres que identifica inequívocamente un recurso (servicio, página, documento, dirección de correo electrónico, enciclopedia, etc).

Normalmente estos recursos son accesibles en una red o sistema basado en el Protocolo IP.

Strip: Los espacios en blanco son despojados de la URI. Este es el comportamiento recomendado por RFC 2396.

Deny: La solicitud es denegada. El usuario recibe un mensaje de "solicitud inválida".

Allow: Se deja que la solicitud y la URI no se cambie. Los espacios en blanco permanecen en el URI.

Encode: e permite que la petición y los espacios en blanco estén codificados de acuerdo con RFC 1738.

Chop: Se permite que la solicitud y la URI se corte en el primer espacio en blanco.

- **Cache Replacement Policy:** La política de sustitución de caché decide qué objetos permanecerán en la memoria caché y qué objetos se sustituyen para crear espacio para los nuevos objetos.

Heap LFUDA: Mantiene los objetos populares en la memoria caché, independientemente de su tamaño y por lo tanto optimiza la tasa de éxito de bytes a expensas de la tasa de éxito.

Heap GDSF: Permite optimizar el índice de aciertos a objetos manteniendo los objetos más pequeños, objetos populares en la memoria caché.

Heap LRU: Funciona como LRU, pero utiliza un montón en su lugar.

LRU: Mantiene recientemente objetos referenciados (es decir, sustituye el objeto que no ha sido visitado por más tiempo).

- **Do Not Cache:** Introduzca dominio (s) y / o dirección IP (es) que nunca deben ser almacenados en caché.
- **Hard Disk Cache Size:** Cantidad de espacio en disco (en megabytes) que se utilizará para los objetos almacenados en caché (no usar más del 50% de la memoria total de nuestro servidor ya que squid siempre en su momento puede usar mas).
- **Hard Disk Cache System:** Esto especifica el tipo de sistema de almacenamiento de usar.

ufs: El viejo conocido formato de almacenamiento de squid que siempre ha estado allí.

- **Minimum Object Size:** Los objetos más pequeños que el tamaño especificado (en kilobytes) no se guardarán en el disco, por defecto: 0 (es decir, no hay un mínimo).
- **Memory Cache Size:** Especifica la cantidad ideal de RAM física (en megabytes) que se utilizará para los objetos en tránsito, objetos calientes y objetos en caché negativo, este valor no debe exceder de 50% de la RAM instalada. El valor mínimo es de 1 MB.
- **Maximum Object Size in RAM:** Objetos mayores que este tamaño (en kilobytes) no se intentarán de mantener en la memoria caché, por defecto: 256 (KB).

- **Memory Replacement Policy:** La política de sustitución de memoria determina qué objetos se limpian de la memoria cuando se necesita espacio.

Heap GDSF: Permite optimizar el índice de aciertos a objetos manteniendo los objetos más pequeños, objetos populares en la memoria caché.

Heap LFUDA: Mantiene los objetos populares en la memoria caché, independientemente de su tamaño y por lo tanto optimiza la tasa de byte de éxito a expensas de la tasa de éxito.

Heap LRU: Funciona como LRU, pero utiliza un montón en su lugar.

LRU: Mantiene recientemente objetos referenciados (es decir, sustituye el objeto que no ha sido visitado por más tiempo). La política de sustitución de memoria determina qué objetos se limpian de la memoria cuando se necesita espacio.

Título 2

Usa los subtítulos consistentemente. Revisando constantemente el espaciado, mayúsculas y puntuación.

Título 3. El uso de estilos es de ayuda a la hora de generar una tabla de contenidos. Este documento de ejemplo usa los títulos, subtítulos y demás estilos para generar automáticamente la tabla de contenido, lista de tablas y lista de figuras. Este documento está configurado para seguir las normas APA.

Título 3. Aquí puede ir otra idea del documento.

Capítulo 2

Usuarios y contraseñas

Nombre-Sistema Operativo	Usuario	Contraseña
Vmware ESXi- Vmware ESXi 5.5		
Proxy Pfsense-Pfsense 2.3.2		