



MANUAL DE INSTALACION Y CONFIGURACION MONOWALL

TRABAJO DE INVESTIGACION

SEGURIDAD INFORMATICA

MANUEL FABRICIO MORA MENDEZ - 1150206

ABSALON EMILIO VERGARA MARTÍNEZ – 1150227

EXAMEN FINAL

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

INGENIERIA DE SISTEMAS

SAN JOSE DE CUCUTA

2012



MONOWALL

m0n0wall es un proyecto destinado a crear un paquete completo de software integrado firewall que, cuando se utiliza junto con un PC integrado, proporciona todas las características importantes de las cajas de cortafuegos comerciales (incluyendo la facilidad de uso) a una fracción del precio (software libre).

m0n0wall se basa en una **versión básica de FreeBSD**, junto con un servidor web, **PHP** y unos servicios públicos de algunos otros. La configuración del sistema se almacena en un único archivo XML de texto para mantener las cosas transparentes.

m0n0wall es probablemente **el primer sistema UNIX que tiene su momento de arranque de configuración realizado con PHP**, en lugar de los scripts de shell habituales, y que tiene **la configuración completa del sistema almacenada en formato XML**.

Características:

En este momento, m0n0wall se puede usar tal cual con ordenadores integrados de los motores de PC y Soekris Ingeniería, o PC más estándar. m0n0wall proporciona muchas de las características de cortafuegos comerciales caros, incluyendo:

- interfaz web (soporta SSL)
- interfaz de la consola de serie para la recuperación
 - configurar la dirección IP de LAN
 - restablecer la contraseña
 - restaurar los valores predeterminados de fábrica
 - reinicio del sistema
- compatibilidad con dispositivos inalámbricos (incluyendo el modo de punto de acceso)
- **portal cautivo**
- **802.1Q VLAN apoyo**
- **Soporte IPv6**
- filtrado de paquetes stateful
 - bloque / pass normas
 - registro
- NAT / PAT (incluyendo 1:1)
- Cliente DHCP, PPPoE y PPTP en la interfaz WAN
- Túneles VPN IPsec (IKE, con soporte para hardware de las tarjetas criptográficas, clientes móviles y certificados)



- PPTP VPN (con soporte RADIUS server)
- rutas estáticas
- Servidor DHCP y relé
- el almacenamiento en caché de DNS forwarder
- DynDNS cliente y RFC 2136 DNS updater
- Agente SNMP
- Traffic Shaper
- SVG basada en el tráfico Grapher
- actualización del firmware a través del navegador web
- Wake on LAN del cliente
- configuración de copia de seguridad / restauración
- host / red alias



webGUI Configuration

m0n0wall.neon1.net

- System**
 - General setup
 - Static routes
 - Firmware
 - Advanced
- Interfaces** (assign)
 - LAN
 - WAN
 - DMZ
 - WLAN
- Firewall**
 - Rules
 - NAT
 - Traffic shaper
 - Aliases
- Services**
 - DNS forwarder
 - Dynamic DNS
 - DHCP server
 - DHCP relay
 - SNMP
 - Proxy ARP
 - Captive portal
 - Wake on LAN
- VPN**
 - IPsec
 - PPTP
- Status**
 - System
 - Interfaces
 - Traffic graph
 - Wireless
- ▶ **Diagnostics**



System information

Name	m0n0wall.neon1.net
Version	1.2 built on Sun Oct 9 18:58:23 CEST 2005
Platform	wrap
Uptime	00:34
Last config change	Mon Oct 10 10:59:55 CEST 2005
CPU usage	view graph
Memory usage	 36%



Especificaciones

- El sistema m0n0wall actualmente ocupa **menos de 5 MB** en una tarjeta Compact Flash o CD-ROM.
- En un net4501, m0n0wall ofrece una WAN <-> LAN TCP rendimiento de alrededor de **17 Mbps** , incluyendo NAT, cuando se ejecuta con la configuración predeterminada. En las plataformas más rápidas (como net4801 o WRAP), el rendimiento de más de 50 Mbps es posible (y hasta a velocidades de gigabit con los nuevos PCs estándar).
- En unas net4501, botas m0n0wall a un estado completamente operativo en menos de **40 segundos** después de la puesta en marcha, incluyendo POST (con un bien configurado la BIOS).

Cómo obtener el software

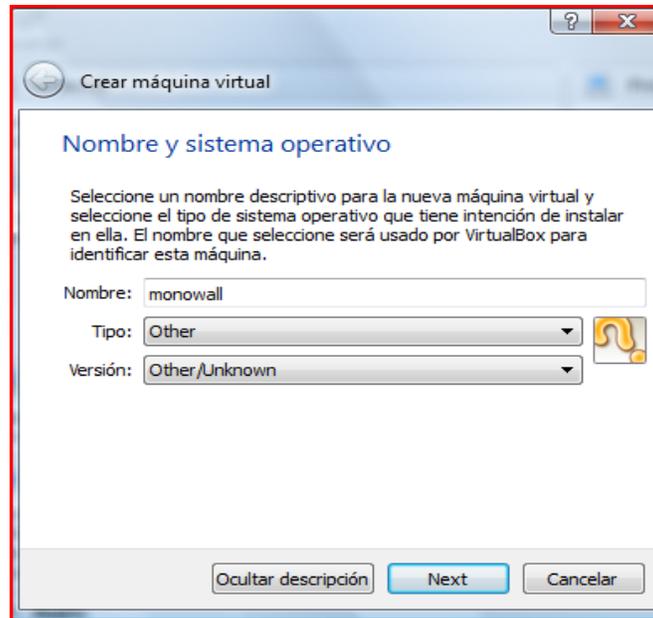
Hay prefabricadas imágenes binarias para los equipos de comunicación de net45xx/net48xx Soekris Ingeniería y la Plataforma Router Wireless Application (WRAP) de motores de PC , una imagen CF / IDE HD para la mayoría de los PC estándar (los integrados pueden funcionar también), una CD-ROM (ISO) por un PC estándar, así como un archivo tar del sistema de ficheros raíz.

Para descargar el software para su plataforma, dirija su navegador web a <http://www.m0n0.ch/wall/downloads.php> y seleccione el vínculo de descarga adecuado de la página.

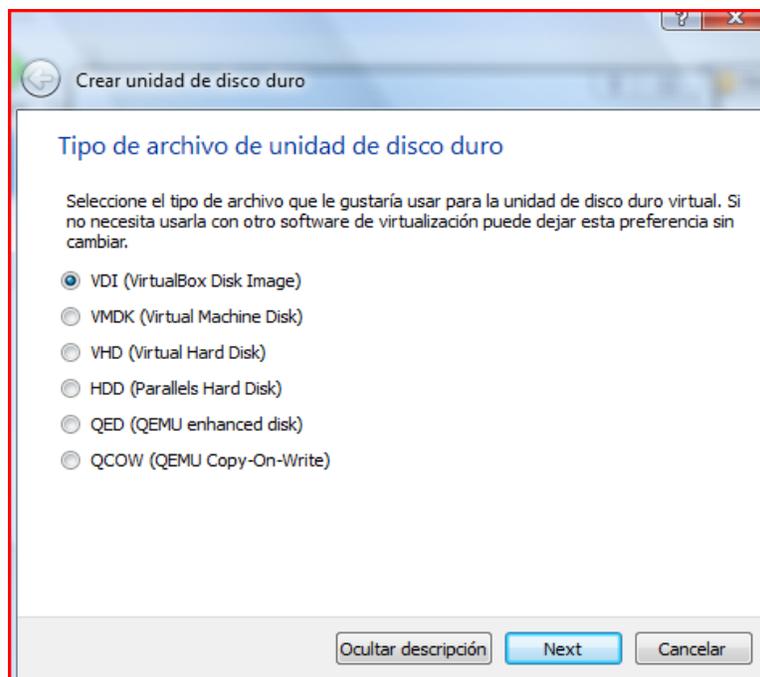
Instalación del Software

m0n0wall está diseñado para arrancar y ejecutar desde una imagen de CD o una tarjeta CompactFlash (CF) o un disco duro IDE. Después de descargar el archivo de imagen apropiado, nos disponemos a crear la maquina virtual en nuestro dropbox previamente instalado.

- Creamos una maquina virtual nueva con nombre monowall.

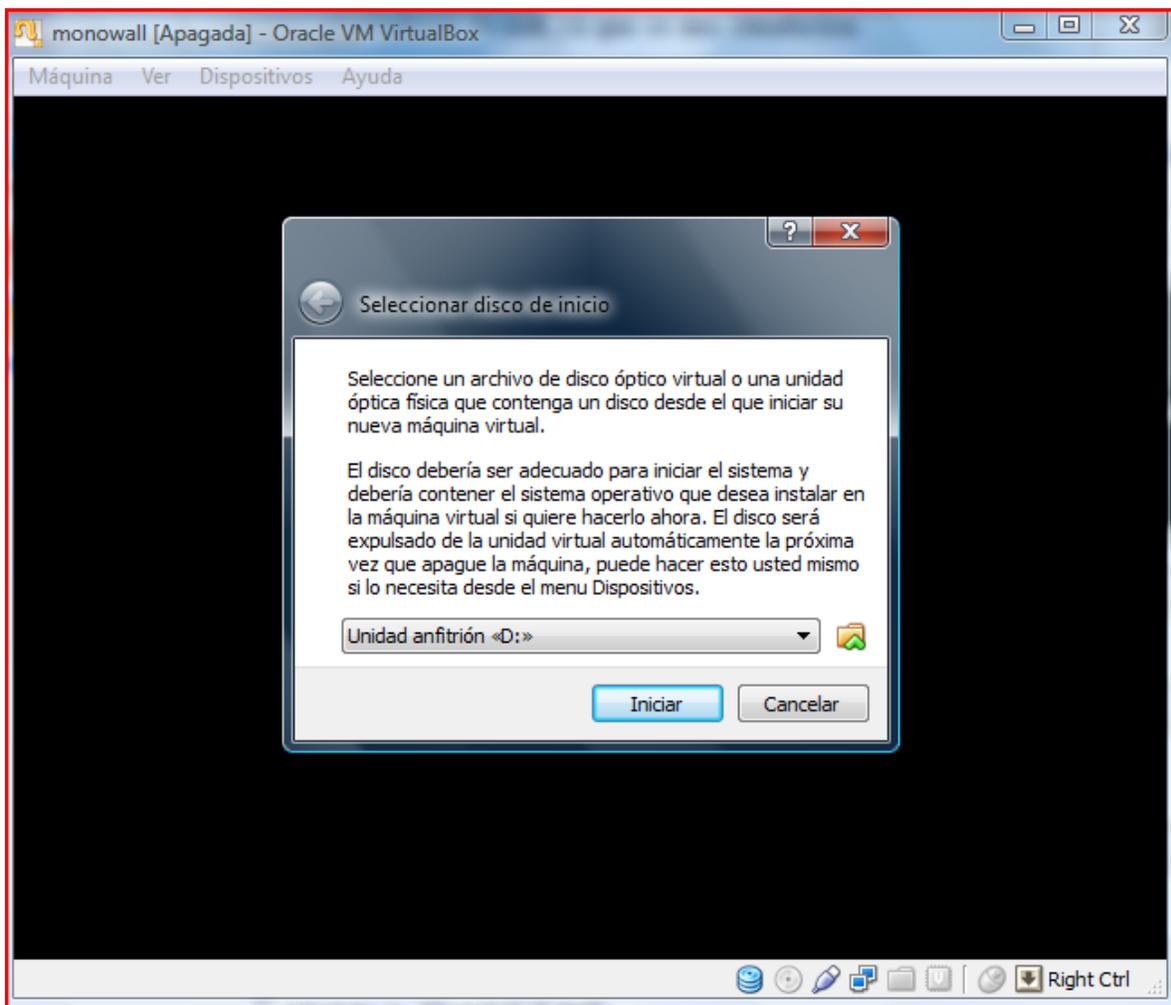


- Damos clic en next, escogemos el tamaño sugerido de 64 mb de memoria, damos clic en next, se selecciona la opción “crear disco virtual ahora”, damos clic en crear. Nos abrirá una nueva ventana para seleccionar el tipo de disco duro virtual.





- Escogemos VDI y damos clic en next , escogemos la opción reservar dinámicamente, tamaño recomendado de 2 gb y por ultimo damos clic en crear.
- Ya con estos pasos esta creada la maquina, ahora hay que iniciarla y seleccionar el archivo .iso de donde se cargará monowall. Nos aparecerá la siguiente pantalla:



- Damos clic en el icono de carpeta y seleccionamos la ubicación y el archivo que fue descargado de instalación. Y damos clic en instalar. El sistema cargará los archivos y nos llevará a una pantalla asi:



```
monowall [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
*** This is m0n0wall, version 1.34
    built on Mon Nov 12 13:17:27 CET 2012 for generic-pc-cdrom
    Copyright (C) 2002-2012 by Manuel Kasper. All rights reserved.
    Visit http://m0n0.ch/wall for updates.

LAN IP address: 192.168.1.1

Port configuration:

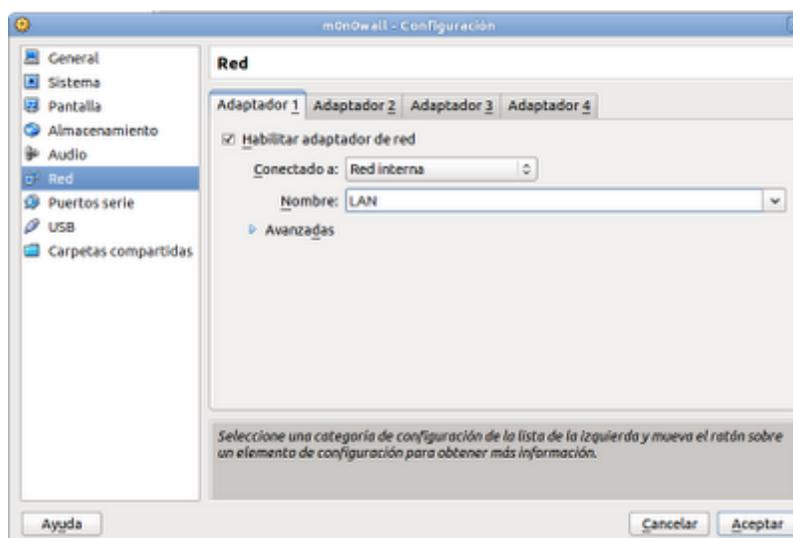
LAN   -> sis0
WAN   -> sis1

m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
7) Install on Hard Drive

Enter a number: |
```

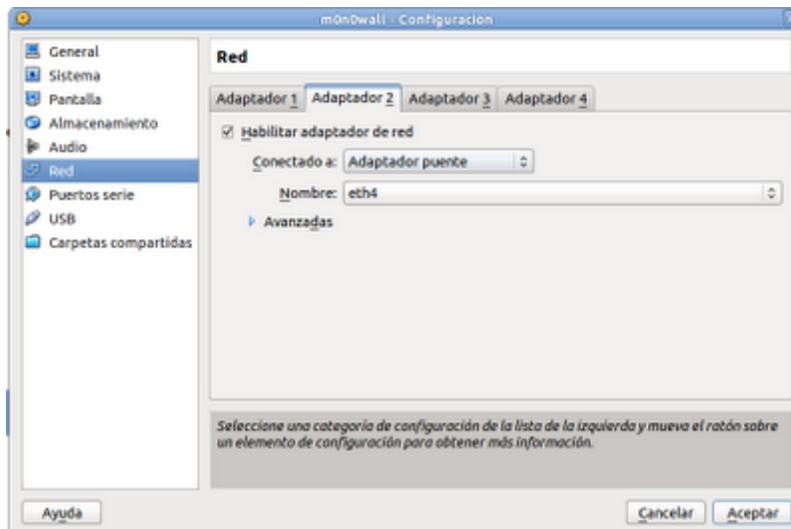
- Apagamos la maquina para configurarle los adaptadores de red. Una vez este apagada, damos clic en propiedades en la maquina.
- Para nuestro firewall (monowall) lo crearemos en una maquina virtual con tres adaptadores de red, ya que es una simulacion. debe haber un adaptado para la LAN otro para la DMZ y otro para la WAN Crearemos nuestros tres adaptadores para nuestro firewall monowall

Para nuestro firewall (monowall) lo crearemos en una maquina virtual con tres adaptadores de red, ya que es una simulación

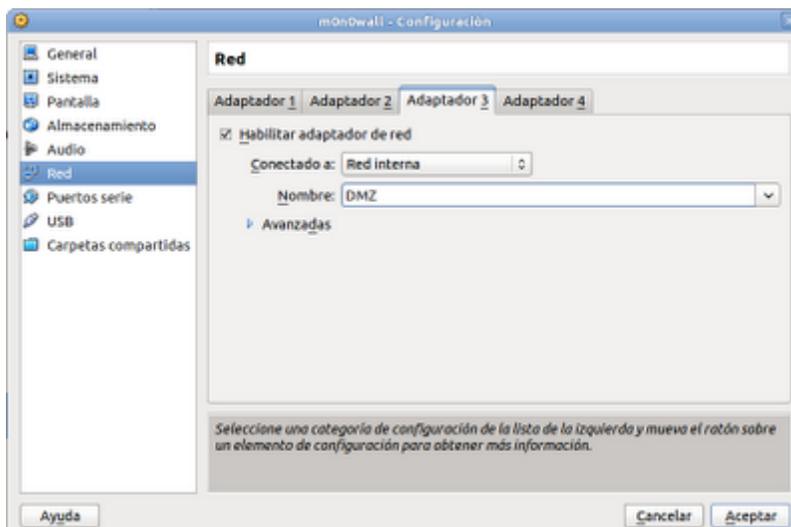




Este adaptador sera red interna con el nombre LAN



El segundo adaptador sera el de nuestra red WAN lo ponemos en adaptador puente y con el nombre por defecto (dependiendo de nuestra conexión)



El tercer adaptador lo configuraremos en red interna con el nombre DMZ, una vez configurados nuestros adaptadores, seguimos con la instalación del monowall.



```
m0n0wall [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
7) Install on Hard Drive
Enter a number: 7
Valid disks are:
sd0    UBOX HARDDISK 1.0    8.00 GB
Enter the device name you wish to install onto: sd0
=====
- WARNING!
- m0n0wall is about to be installed onto the sd0 device.
- - everything on this device will be erased!
- - this cannot be undone!
=====
The firewall will reboot after installation.
Do you want to proceed? (y/n) y
```

esta parte ponemos el nombre de nuestro disco, que nos parece después de darle la opción 7, y luego confirmamos con y

```
m0n0wall [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
WAN -> sisl

m0n0wall console setup
=====
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
Enter a number: 1
Valid interfaces are:
em0    08:00:27:e8:2d:5c    (up)    Intel(R) PRO/1000 Network Connection Ver...
em1    08:00:27:8a:54:60    (up)    Intel(R) PRO/1000 Network Connection Ver...
em2    08:00:27:b1:5a:5f    (up)    Intel(R) PRO/1000 Network Connection Ver...
Do you want to set up VLANs first?
If you're not going to use VLANs, or only for optional interfaces, you
should say no here and use the webGUI to configure VLANs later, if required.
Do you want to set up VLANs now? (y/n) n
```

Ahora asignaremos las interfaces, le damos la opción 1, y si queremos configurar interfaces de VLAN le damos y, en este caso como no tenemos le damos n



```
m0n0wall [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
Do you want to set up VLANs now? (y/n) n

If you don't know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces before you begin,
and reconnect each one when prompted to do so.

Enter the LAN interface name or 'a' for auto-detection: em0
Enter the WAN interface name or 'a' for auto-detection: em1
Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished): em2
Enter the Optional 2 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:
LAN -> em0
WAN -> em1
OPT1 -> em2

The firewall will reboot after saving the changes.
Do you want to proceed? (y/n) y
```

luego de esto empezamos a ingresar el nombre de cada interfaz, que como podemos ver nos salió al principio después de darle la opción 1, agregamos una por una y confirmamos con y.

```
m0n0wall [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: em0: watchdog timeout -- resetting
5

Enter a host name or IP address: 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=47 time=80.785 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=47 time=83.347 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=47 time=80.047 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 80.047/81.393/83.347/1.414 ms

Press ENTER to continue.
```

Ahora haremos un ping a internet, seleccionando la opción 6, ping 8.8.8.8, si es exitoso proseguimos, si no verificaremos nuestras conexiones, hasta que sea exitoso.



```
m0n0wall [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
WAN -> em1
OPT1 -> em2 (OPT1)

m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: 2

Enter the new LAN IP address: 192.168.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in m0n0wall.
e.g. 255.255.255.0 = 24
    255.255.0.0   = 16
    255.0.0.0     = 8

Enter the new LAN subnet bit count: 24

Do you want to enable the DHCP server on LAN? (y/n) y
```

En este paso le daremos la opción 2 para configurar un dhcp en la LAN, si queremos cambiamos la dirección de nuestro monowall o dejamos la que por defecto tiene poniendo 192.168.1.1.

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the client address range: 192.168.1.2
Enter the end address of the client address range: 192.168.1.10
```

Damos el rango que usaremos y listo. Desde un equipo en nuestra lan verifiquemos haciendo un ping a la interfaz LAN del monowall que por defecto es la 192.168.1.1, si es exitoso abrimos la interfaz web de mono wall poniendo esta dirección en nuestra barra de dirección.





Si nos pide login, el login por defecto es **admin** y la contraseña **mono**.

Configuración de interfaces

Si queremos cambiar la dirección de nuestra LAN nos dirigimos a interfaces y seleccionamos LAN, y la cambiamos, lo mismo para la WAN, y para la DMZ hacemos click en OPT1 (interfaz opcional) y la habilitamos, le cambiamos el nombre si queremos en Description, y agregamos una dirección ip para nuestra interfaz de la siguiente manera.



Aquí ya asignamos el nombre, la habilitamos y le asignamos una dirección ip la 192.168.2.1.

Configuración del NAT

Tenemos los servicios ftp y web en la DMZ para que sean accesibles para todos, y los de la LAN (ftp y web) son privados, y no podemos acceder a ellos desde ningún host fuera de la red, entonces para que los servicios de nuestra DMZ sean accesibles configuraremos las reglas del NAT de la siguiente manera.



System General setup Static routes Firmware Advanced User manager	Firewall: NAT: Edit
Interfaces (assign) LAN WAN	Interface WAN Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Firewall Rules NAT Traffic shaper Aliases	External address Interface address If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define IP addresses on the Server NAT page first).
Services DNS forwarder Dynamic DNS DHCP server DHCP relay SNMP Proxy ARP Captive portal Wake on LAN	Protocol TCP Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
VPN IPsec PPTP	External port range from: (other) <input type="text"/> to: (other) <input type="text"/> Specify the port or port range on the firewall's external address for this mapping. Hint: you can leave the 'to' field empty if you only want to map a single port
Status System Interfaces Traffic graph Wireless	NAT IP 192.168.2.2 Enter the internal IP address of the server on which you want to map the ports. e.g. <i>192.168.1.12</i>
▶ Diagnostics	Local port FTP Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above
	Description ftp a dmz You may enter a description here for your reference (not parsed).
	<input type="checkbox"/> Auto-add a firewall rule to permit traffic through this NAT rule
	Save

m0n0wall@is © 2002-2012 by Manuel Kasper. All rights reserved. [view license]

TCP o el protocolo por el que corra nuestro servicio, en external port range el puerto externo, en NAT IP la dirección a la cual serán redireccionadas las peticiones en este caso la de la DMZ y en local port el puerto local y si queremos una descripción al final.

Crearemos otra regla igual pero esta vez para nuestro servicio WEB, solo cambiando los puertos a HTTP.



System

- General setup
- Static routes
- Firmware
- Advanced
- User manager

Interfaces (assign)

- LAN
- WAN

Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN

Firewall: NAT: Inbound



The NAT configuration has been changed.
You must apply the changes in order for them to take effect.

Apply changes

- Inbound
- Server NAT
- 1:1
- Outbound

	If	Proto	Ext. port range	NAT IP	Int. port range	Description	
<input type="checkbox"/>	WAN	TCP	21 (FTP)	192.168.2.2	21 (FTP)	ftp a dmz	⊞
<input type="checkbox"/>	WAN	TCP	80 (HTTP)	192.168.2.2	80 (HTTP)	web a dmz	⊞

Note:

It is not possible to access NATed services using the WAN IP address from within LAN (or an optional network).

Y tendremos dos reglas en el NAT una para el FTP y otra para el WEB que permitirán el acceso a estos desde un host en la WAN.



- System
 - General setup
 - Static routes
 - Firmware
 - Advanced
 - User manager
- Interfaces (assign)
 - LAN
 - WAN
- Firewall
 - Rules
 - NAT
 - Traffic shaper
 - Aliases
- Services
 - DNS forwarder
 - Dynamic DNS
 - DHCP server
 - DHCP relay
 - SNMP
 - Proxy ARP
 - Captive portal
 - Wake on LAN
- VPN
 - IPsec
 - PPTP
- Status
 - System
 - Interfaces
 - Traffic graph
 - Wireless
- ▶ Diagnostics

Firewall: Traffic shaper: Rules

Rules Pipes Queues Magic shaper wizard

Enable traffic shaper

Save

If	Proto	Source	Destination	Target	Description
----	-------	--------	-------------	--------	-------------



- incoming (as seen by firewall) ← outgoing (as seen by firewall)
- incoming (disabled) ← outgoing (disabled)

Note:
the first rule that matches a packet will be executed.
The following match patterns are not shown in the list above: IP packet length, TCP flags.

Activamos el portal cautivo para poder autenticar.



Services: Captive portal

Captive Portal	Pass-through MAC	Allowed IP addresses	Users	Vouchers	File Manager
<input checked="" type="checkbox"/> Enable captive portal					
Interface	LAN <input type="button" value="v"/> Choose which interface to run the captive portal on.				
Maximum concurrent connections	<input type="text"/> per client IP address (0 = no limit) <input type="text"/> total This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Default is 4 connections per client IP address, with a total maximum of 16 connections.				
Idle timeout	<input type="text"/> minutes Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.				
Hard timeout	60 <input type="text"/> minutes Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).				
Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.				
Redirection URL	<input type="text" value="crcciudaddetodos.org"/> If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.				
Concurrent user logins	<input type="checkbox"/> Disable concurrent logins If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.				

En redirection URL escribimos una pagina web a la cual queremos que el cliente quiera ser redireccionado después de intentar conectarse a internet.

Ahora podemos restringir el ancho de banda para los usuarios y adicionalmente habilitar la opción para tener que iniciar sesión para ingresar a la red.



Per-user bandwidth restriction	<input checked="" type="checkbox"/> Enable per-user bandwidth restriction Default download <input type="text" value="1000"/> Kbit/s Default upload <input type="text" value="1000"/> Kbit/s <p>If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. RADIUS can override the default settings. Leave empty or set to 0 for no limit. You will need to enable the traffic shaper for this to be effective.</p>
Authentication	<p><input type="radio"/> No authentication <input checked="" type="radio"/> Local user manager <input type="radio"/> RADIUS authentication</p> <p>Primary RADIUS server</p> <p>IP address <input type="text"/> Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.</p> <p>Port <input type="text"/> Leave this field blank to use the default port (1812).</p> <p>Shared secret <input type="text"/> Leave this field blank to not use a RADIUS shared secret (not recommended).</p>

Los usuarios y sus claves son administradas en User manager

Services: Captive portal: Edit user

Username	<input type="text" value="absalon"/>
Password	<input type="password" value="....."/> <input type="password" value="....."/> (confirmation)
Full name	<input type="text" value="absalon"/> User's full name, for your own information only
Expiration date	<input type="text" value="3/6/2013"/> Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy



La anterior imagen muestra como podemos crear un usuario con su respectiva clave y fecha de caducidad el usuario. Damos clic en Save para guardar cambios.