

2012

# ENDIAN FIREWALL

## INSTALACION Y CONFIGURACION

ES UNA DISTRIBUCION GNU/LINUX LIBRE ESPECIALIZADA EN CORTAFUEGOS (FIREWALL), RUTEO Y GESTION UNIFICADA DE AMENAZAS. ENDIAN FIREWALL ES UNA LLAVE EN MANO QUE CONVIERTE A TODO EL SISTEMA EN UN DISPOSITIVO DE SEGURIDAD CON TODAS LAS FUNCIONES CON GESTION UNIFICADA DE AMENAZAS (UTM) FUNCIONALIDAD.

**CENTRO DE SERVICIOS Y GESTION EMPRESARIAL  
CESGE**

**SERVICIO NACIONAL DE APRENDIZAJE SENA**

**INSTRUCTOR**

**JULIAN CIRO**

**ADMINISTRACION DE REDES #230490**

**MEDELLIN-ANTIOQUIA**

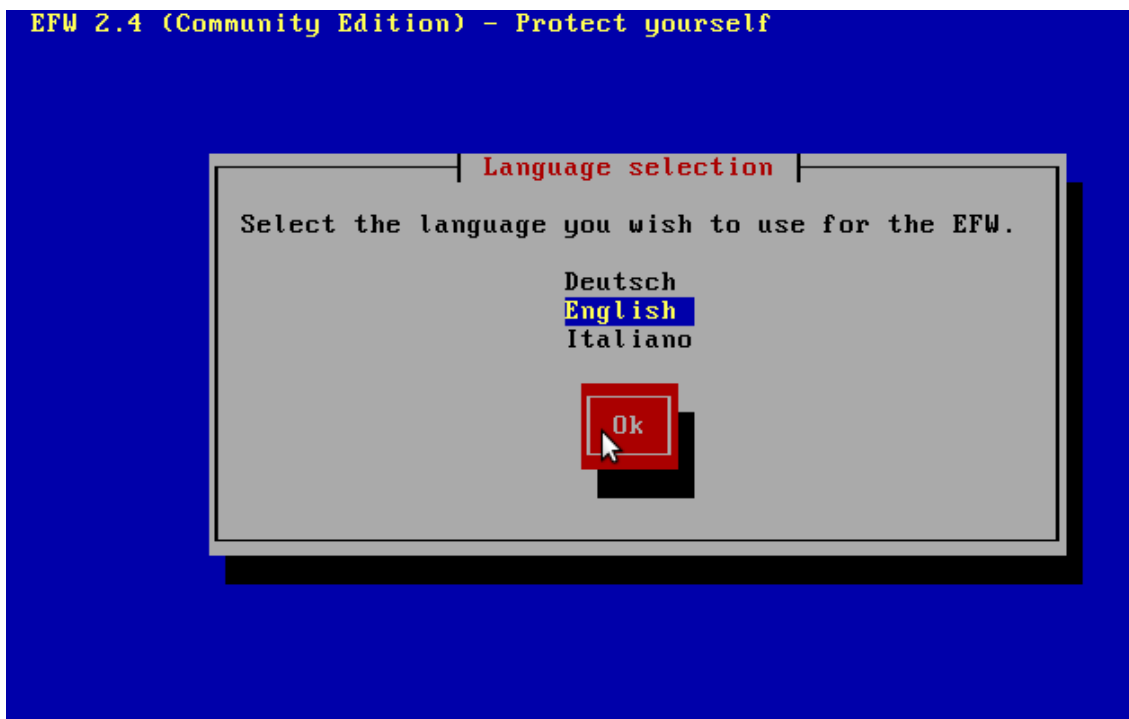
BRENDA TOVAR-----DEYANIRA CARATAR  
06/11/2012



## ENDIAN FIREWALL

### 1. Instalando endian firewall.

Elegimos el idioma-ok.

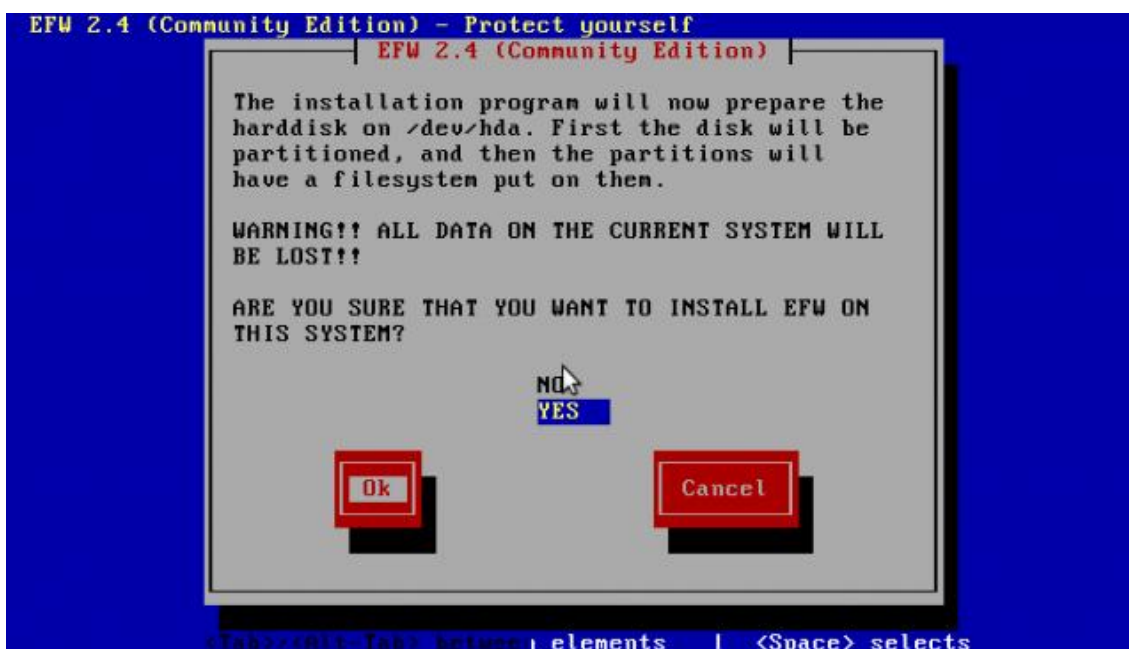


### 2. Nos muestra un mensaje de bienvenida para la instalación de endian-ok.



### 3. Advertencia, especifica que el proceso de instalación borrara todos los datos que contenga el disco duro-YES.

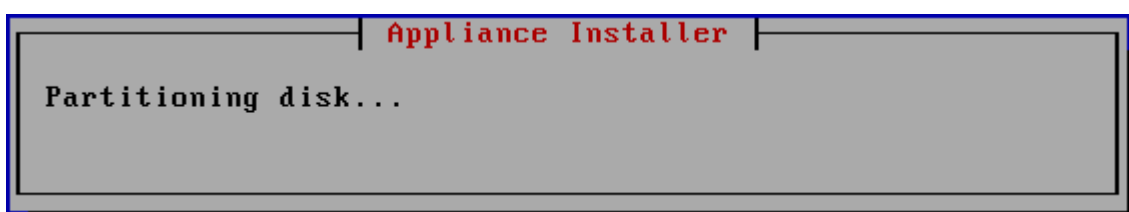
## ENDIAN FIREWALL



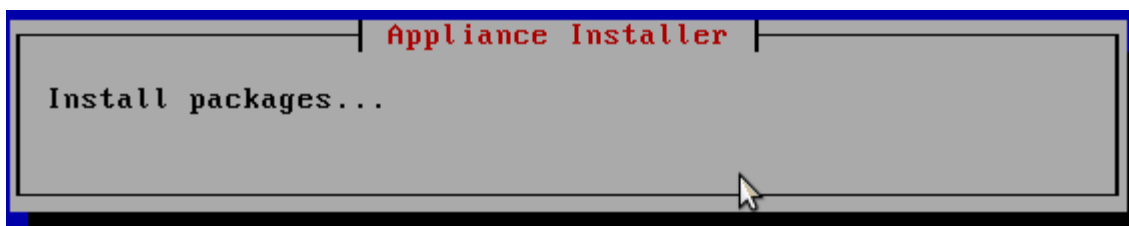
4. Nos da la opción de elegir si queremos el servicio de consola, la elegimos según, la necesidad.



5. Ahora endian comienza a instalarse en nuestro disco.



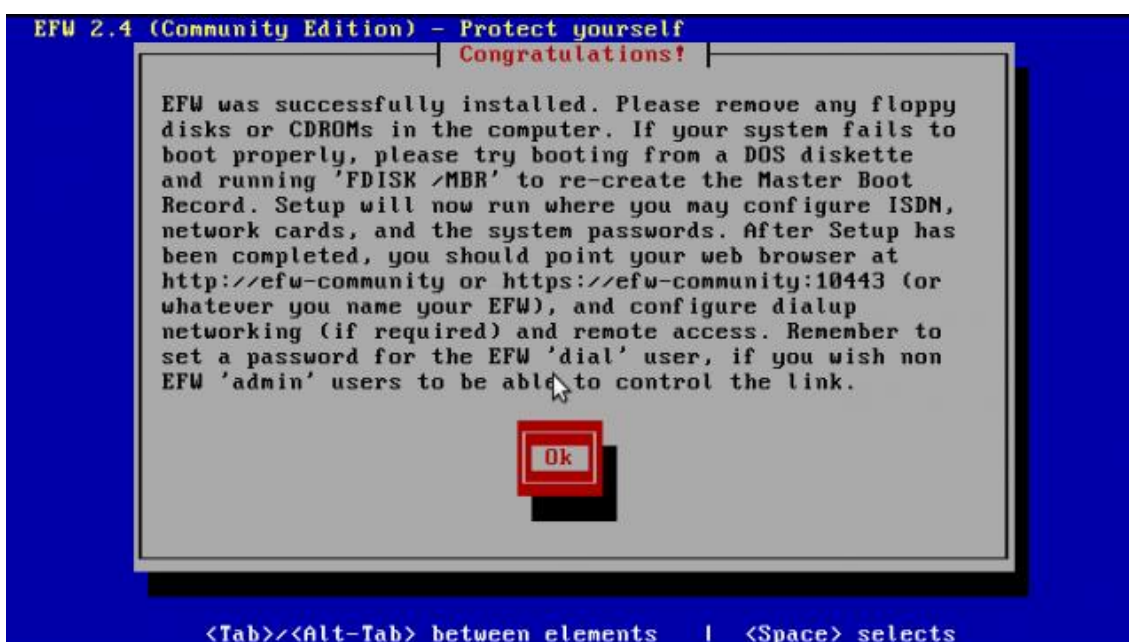
## ENDIAN FIREWALL



6. Ahora debemos darle la IP al endian.



7. Se recomienda quitar cualquier diskette o CD-ROM que aún se encuentre insertado, damos OK para que el sistema se reinicie.



8. Luego de reiniciarse, aparecerán las opciones que usted necesite.

## ENDIAN FIREWALL

```
Release: Endian Firewall Community release 2.4.0

Management URL: https://192.168.30.1:10443
Green IP       : 192.168.30.1/None
-----

0) Shell
1) Reboot
2) Change Root Password
3) Change Admin Password
4) Restore Factory Defaults

Choice: _
```

9. Debemos tener en cuenta que endian debe tener tres adaptadores de red con diferentes nombres y direccionamiento, nosotros tenemos, en adaptador 1: LAN, adaptador 2: dmz, y adaptador 3: out en red interna todos.

```
root@firewall:~ # ifconfig
br0      Link encap:Ethernet  HWaddr 08:00:27:72:4E:49
         inet addr:192.168.30.1  Bcast:192.168.30.255  Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fe72:4e49/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:25890 errors:0 dropped:0 overruns:0 frame:0
         TX packets:34539 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:2357862 (2.2 MiB)  TX bytes:18174568 (17.3 MiB)

br1      Link encap:Ethernet  HWaddr 08:00:27:BB:D5:33
         inet addr:192.168.20.1  Bcast:192.168.20.255  Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:febb:d533/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:1606 errors:0 dropped:0 overruns:0 frame:0
         TX packets:1537 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:123527 (120.6 KiB)  TX bytes:133712 (130.5 KiB)
```

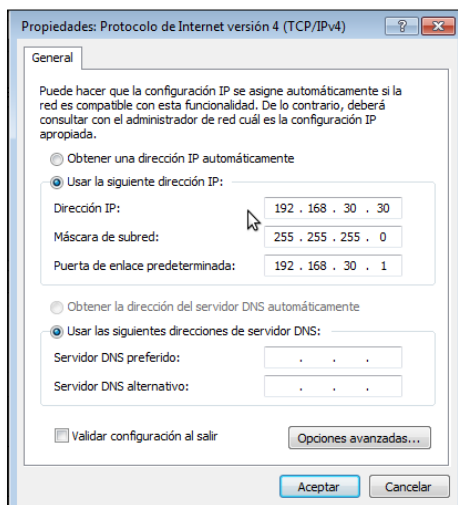
```
eth2     Link encap:Ethernet  HWaddr 08:00:27:A9:FA:A3
         inet addr:209.165.200.1  Bcast:209.165.200.255  Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fea9:faa3/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:2191 errors:0 dropped:0 overruns:0 frame:0
         TX packets:2406 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:450175 (439.6 KiB)  TX bytes:299826 (292.7 KiB)

lo       Link encap:Local Loopback
         inet addr:127.0.0.1  Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING  MTU:16436  Metric:1
         RX packets:31210 errors:0 dropped:0 overruns:0 frame:0
         TX packets:31210 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:6773701 (6.4 MiB)  TX bytes:6773701 (6.4 MiB)
```

10. Abrimos una máquina virtual, Windows 7, esta es la red inside.

## ENDIAN FIREWALL

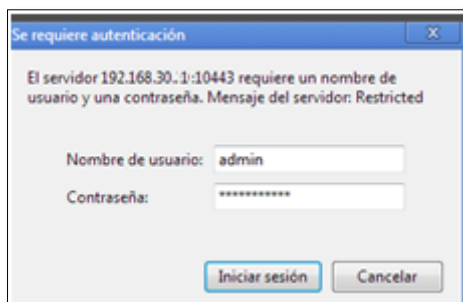
Recordemos que la 192.168.30.1 es la ip del endian, y en nuestra máquina virtual inside o quien desee que sea el modo grafico del endian.



11. Nos vamos al navegador y escribimos en la url, la dirección que posee el endian.

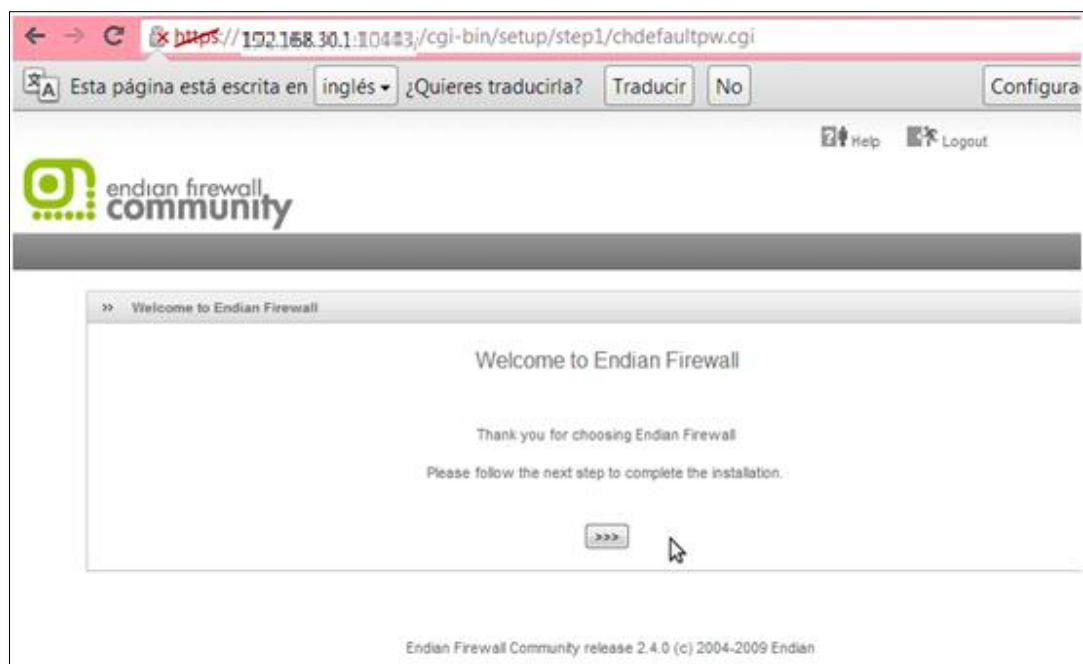


12. Nos aparece las credenciales de usuario para ingresar al modo grafico del endian.

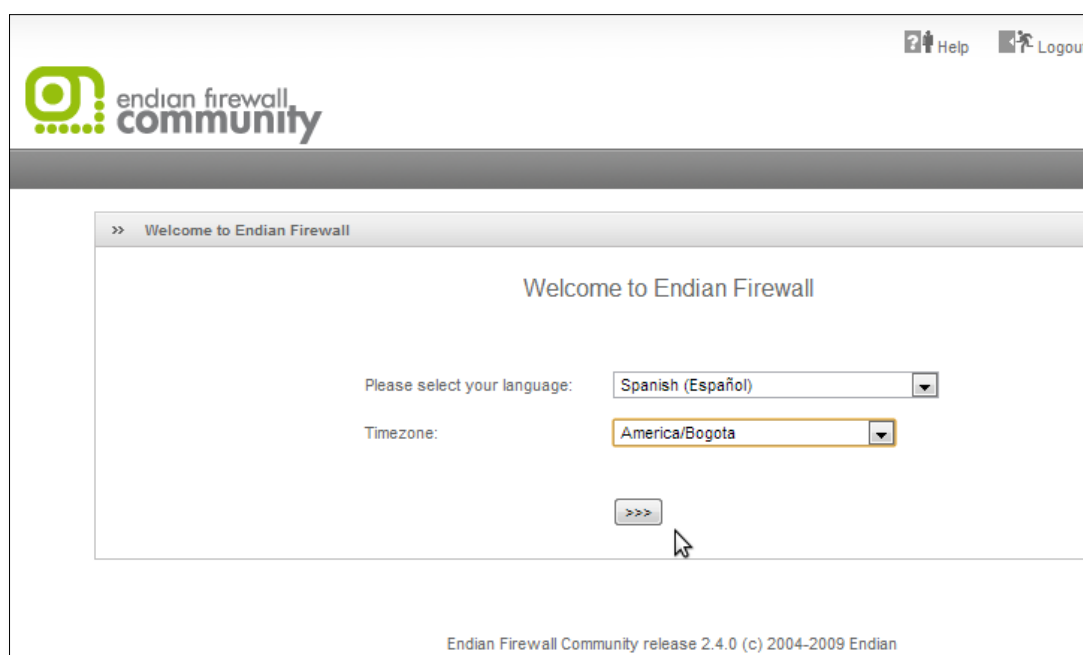


13. .nos da la bienvenida al firewall endian, le damos clic en “>>>”.

## ENDIAN FIREWALL



**14. Nos da la opción de elegir el idioma y la zona horario, clic >>>**



**15. Aceptamos las condiciones del contrato, clic >>>**

## ENDIAN FIREWALL

Welcome to Endian Firewall

---

GNU GENERAL PUBLIC LICENSE  
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.  
51 Franklin St, Fifth Floor, Boston, MA 02110-1301  
USA

Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your  
freedom to share and change it. By contrast, the GNU General Public  
License is intended to guarantee your freedom to share and change free  
software--to make sure the software is free for all its users. This  
General Public License applies to most of the Free Software  
Foundation's software and to any other program whose authors commit to  
using it. (Some other Free Software Foundation software is covered by  
the GNU Library General Public License instead.) You can apply it to  
your programs, too.

ACCEPT License

>>>

16. Como no tenemos un respaldo, decimos no, clic >>>

Ayuda Cerrar sesión

 endian firewall community

---


>> Importar respaldo

¿Desea restaurar un respaldo?

Endian Firewall Community release 2.4.0 (c) 2004-2009 Endian

17. Le damos las contraseñas a esos servicios clic >>>

Ayuda Cerrar sesión

 endian firewall community

---

>> Cambiar la Contraseña por Defecto

<p>Contraseña (admin) de la interfaz web</p> <p>Contraseña *</p> <input type="password"/> <p>Confirmar Contraseña *</p> <input type="password"/>	<p>Contraseña (root) SSH</p> <p>Contraseña *</p> <input type="password"/> <p>Confirmar Contraseña *</p> <input type="password"/>
--	--

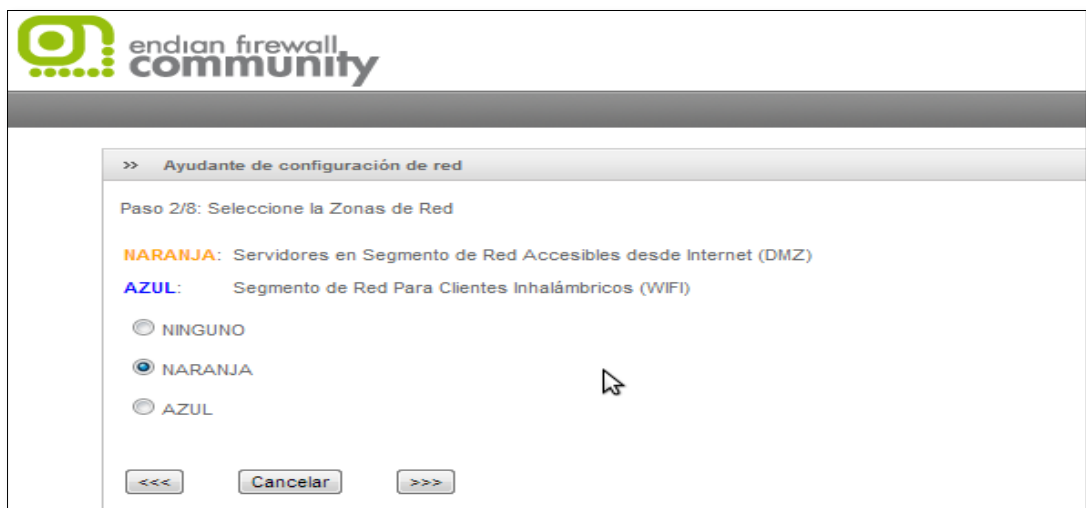
Endian Firewall Community release 2.4.0 (c) 2004-2009 Endian



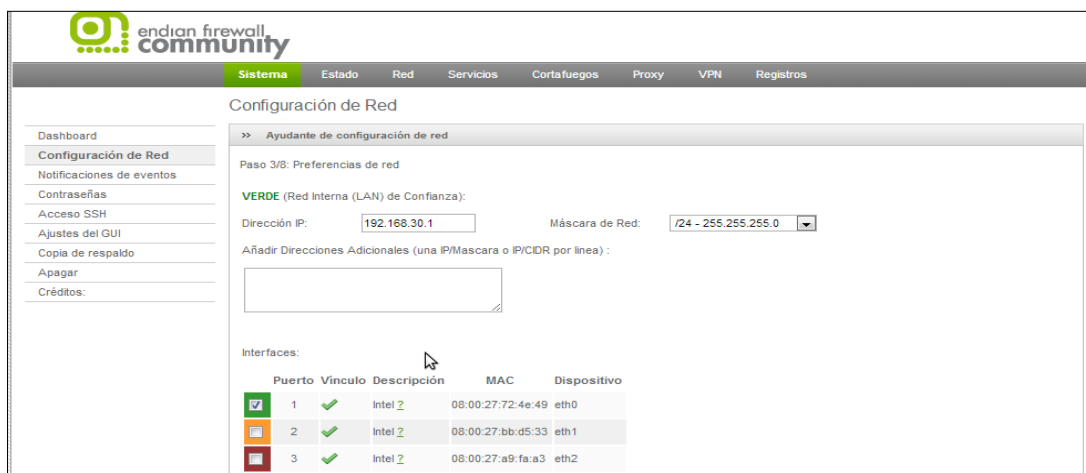
18. Como le daremos una ip estática a la zona roja “outside” clic >>>



19. Elegimos la interfaz a configurar clic >>>



20. Le damos el Gateway de la zona verde “inside”



## 21. Le damos el Gateway de la zona naranja “dmz”

**NARANJA** (Servidores en Segmento de Red Accesibles desde Internet (DMZ)):

Dirección IP:  Máscara de Red:

Añadir Direcciones Adicionales (una IP/Mascara o IP/CIDR por linea) :

Interfaces:

Puerto	Vínculo	Descripción	MAC	Dispositivo
1	<input checked="" type="checkbox"/>	Intel 2	08:00:27:72:4e:49	eth0
2	<input checked="" type="checkbox"/>	Intel 2	08:00:27:bb:d5:33	eth1
3	<input checked="" type="checkbox"/>	Intel 2	08:00:27:a9:fa:a3	eth2

Nombre del Anfitrión:

Nombre del Dominio:

<<<  >>>

## 22. Le damos el Gateway de la zona roja “outside”

**ROJA** (Conexión a Internet (WAN), no Confiable):

Dirección IP:  Máscara de Red:

Añadir Direcciones Adicionales (una IP/Mascara o IP/CIDR por linea) :

Interfaces:

Puerto	Vínculo	Descripción	MAC	Dispositivo
1	<input checked="" type="checkbox"/>	Intel 2	08:00:27:72:4e:49	eth0
2	<input checked="" type="checkbox"/>	Intel 2	08:00:27:bb:d5:33	eth1
3	<input checked="" type="checkbox"/>	Intel 2	08:00:27:a9:fa:a3	eth2

Puerta de enlace predeterminada:

MTU:

"Spoof" la dirección MAC con:

Este campo puede quedar en blanco

23. En este caso, yo le puse como dns el mismo, el Gateway del a zona roja “outside”.

**Configuración de Red**

>> **Ayudante de configuración de red**

Paso 5/8: Configurar DNS

Configuración Manual DNS:

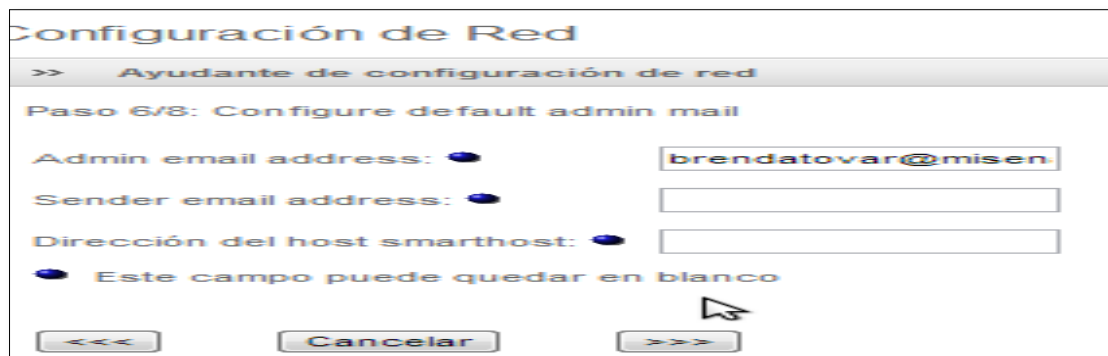
DNS 1:

DNS 2:

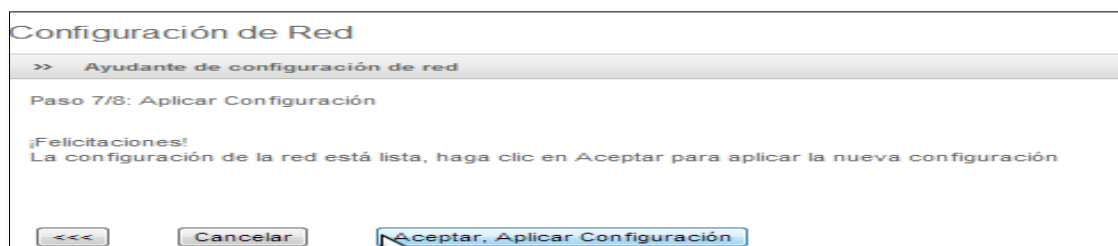
<<<  >>>

24. Esto es opcional, no es obligatorio, todo lo que tenga puntitos azules son campos que están en decisión nuestra de llenarlos o no.

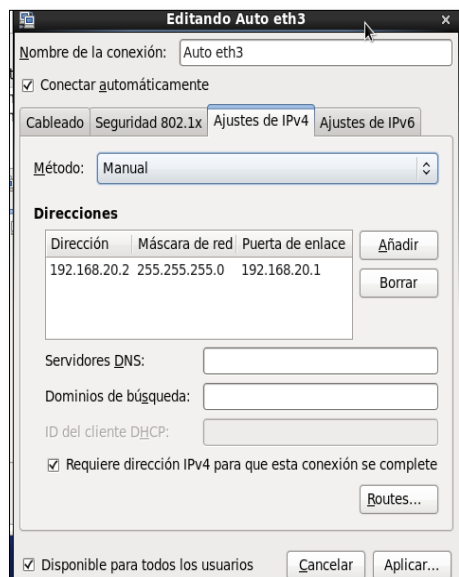
## ENDIAN FIREWALL



**25. Finalizamos el proceso de configuración de red, aplicamos los cambios.**



**26. Ahora procedemos a configurar las otras dos máquinas virtuales, en centos "dmz", en Windows xp "outside", recuerdo que todos deben estar en red interna.**

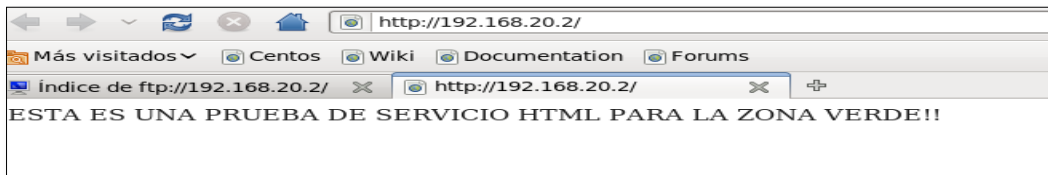
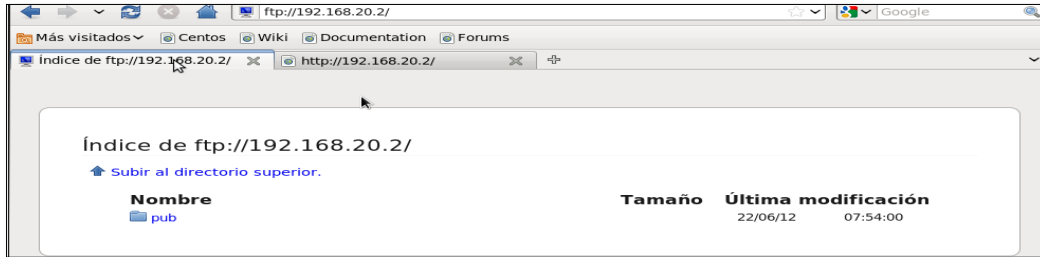


**27. Configuramos los servicios en la dmz, http (protocolo de transferencias de hipertexto), y ftp (protocolo de transferencia de archivos).**

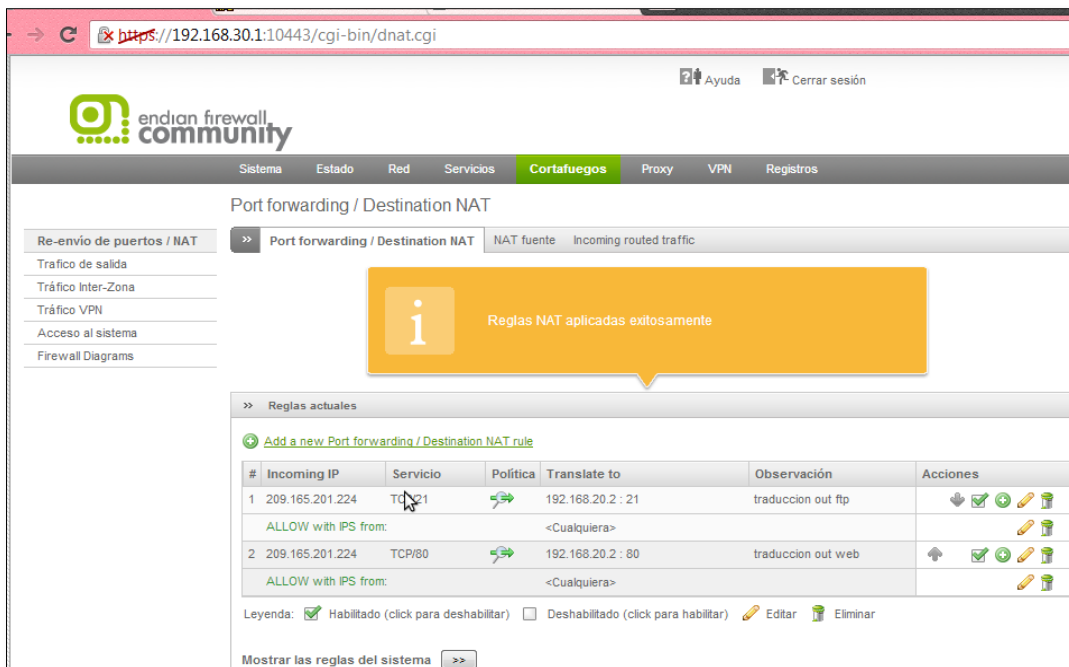
## ENDIAN FIREWALL

```
root@localhost:~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
[root@localhost Escritorio]# service httpd restart
Parando httpd: [ OK ]
Iniciando httpd: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain for ServerName [ OK ]
[root@localhost Escritorio]# service vsftpd restart
Apagando vsftpd: [ OK ]
Iniciando vsftpd para vsftpd: [ OK ]
[root@localhost Escritorio]#
```

28. Abrimos el explorador en centos, escribiendo ftp y http, con su IP.



29. Nos dirigimos a Windows 7, al modo gráfico del endian; en port forwarding/destination NAT nos permite traducir la ip interna (privada) a una ip externa (publica), especificando los puertos.



30. Esta es la forma en que se crea las reglas, esto es para el ftp, como ip entrante “la pública” y que traduzca como la dirección ip del dmz (zona naranja).

## ENDIAN FIREWALL

The screenshot shows the 'Port forwarding / Destination NAT' configuration page in the Endian Firewall web interface. The 'Cortafuegos' menu is active. The page title is 'Port forwarding / Destination NAT'. The left sidebar contains navigation options: 'Re-envío de puertos / NAT', 'Tráfico de salida', 'Tráfico Inter-Zona', 'Tráfico VPN', 'Acceso al sistema', and 'Firewall Diagrams'. The main content area is titled 'Reglas actuales' and contains a 'Port forwarding / Destination NAT Rule Editor' form. The form is in 'Simple Mode' and has the following fields:

- Incoming IP:** Tipo \* 'Red/IP/Rango', Introduce los IPs/red (uno por línea) '209.165.201.224'.
- Incoming Service/Port:** Servicio \* 'FTP', Incoming port/range (one per line, e.g. 80, 80:88) '21', Protocolo \* 'TCP'.
- Translate to \*:** Insertar IP '192.168.20.2', Port/Range (e.g. 80, 80:88) '21', NAT 'NAT'.
- Options:**  Activado,  Registro, Observación 'traduccion out ftp', Posición \* 'Primero'.

Buttons: 'Actualizar Regla' and 'Cancelar'. A note at the bottom right states: '\* Este campo es obligatorio.'

**31. Lo mismo hacemos para el http, damos la dirección ip entrante la outside (zona roja), y que lo traduzca a la ip del dmz (zona naranja).**

The screenshot shows the 'Port forwarding / Destination NAT' configuration page in the Endian Firewall web interface. The 'Cortafuegos' menu is active. The page title is 'Port forwarding / Destination NAT'. The left sidebar contains navigation options: 'Re-envío de puertos / NAT', 'Tráfico de salida', 'Tráfico Inter-Zona', 'Tráfico VPN', 'Acceso al sistema', and 'Firewall Diagrams'. The main content area is titled 'Reglas actuales' and contains a 'Port forwarding / Destination NAT Rule Editor' form. The form is in 'Simple Mode' and has the following fields:

- Incoming IP:** Tipo \* 'Red/IP/Rango', Introduce los IPs/red (uno por línea) '209.165.201.224'.
- Incoming Service/Port:** Servicio \* 'HTTP', Incoming port/range (one per line, e.g. 80, 80:88) '80', Protocolo \* 'TCP'.
- Translate to \*:** Insertar IP '192.168.20.2', Port/Range (e.g. 80, 80:88) '80', NAT 'NAT'.
- Options:**  Activado,  Registro, Observación 'traduccion out web', Posición \* 'Después de la Regla #1'.

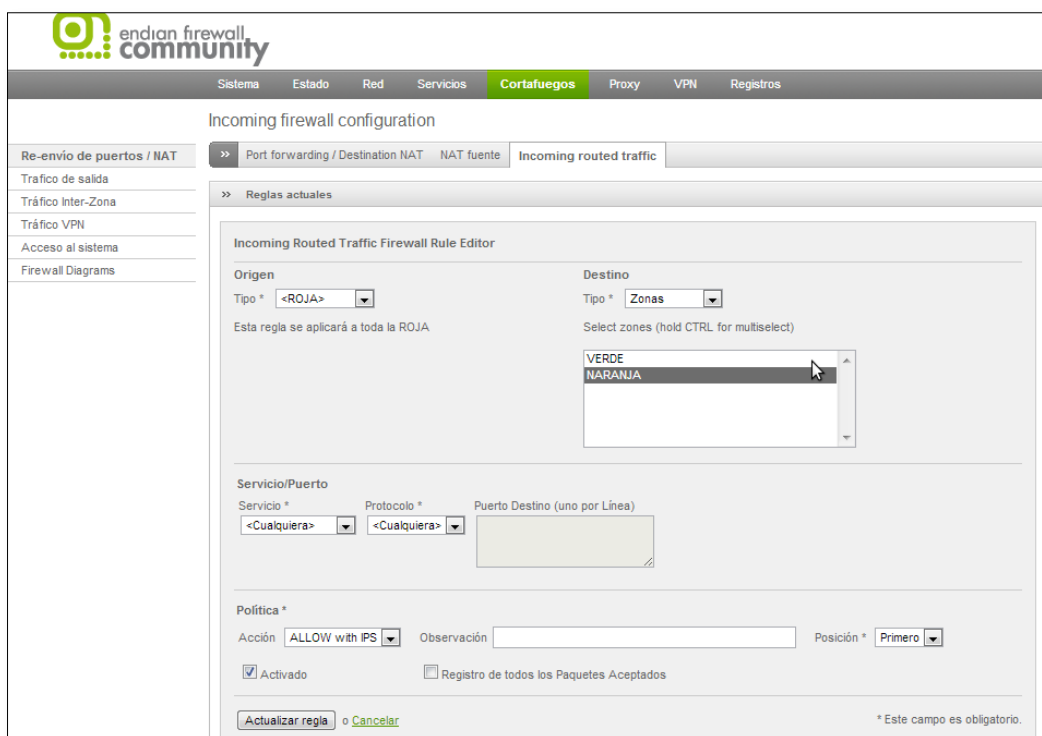
Buttons: 'Actualizar Regla' and 'Cancelar'. A note at the bottom right states: '\* Este campo es obligatorio.'

**32. Nos dirigimos al incoming routed traffic, y creamos una regla diciendo, que cualquier origen con destino a la zona roja (outside), con cualquier servicio lo permita.**

## ENDIAN FIREWALL



**33. Esta es la manera en que se crea la regla para el tráfico entrante al route.**



**34. Le damos clic en crear regla, aplicar, y nos saldrá el letrero naranja diciendo que los cambios han sido aplicadas correctamente.**

**La regla que vemos abajo, la editaremos adelante.**

## ENDIAN FIREWALL

i Las reglas de cortafuegos fueron aplicadas exitosamente

>> Reglas actuales

[Agregar una nueva regla del cortafuegos](#)

#	Origen	Destino	Servicio	Política	Observación	Acciones
1	192.168.30.30/24	209.165.200.200/24	TCP/8080	→	hyt	⬆️ ✓ ✎ 🗑️
2	VERDE	ROJA	TCP/80	→		⬆️ ⬆️ ✓ ✎ 🗑️
3	VERDE	ROJA	TCP/80	→	allow HTTP	⬆️ ⬆️ ✓ ✎ 🗑️
4	VERDE AZUL	ROJA	TCP/443	→	allow HTTPS	⬆️ ⬆️ ✓ ✎ 🗑️
5	VERDE	ROJA	TCP/21	→	allow FTP	⬆️ ⬆️ ✓ ✎ 🗑️
6	VERDE	ROJA	TCP/25	→	allow SMTP	⬆️ ⬆️ ✓ ✎ 🗑️
7	VERDE	ROJA	TCP/110	→	allow POP	⬆️ ⬆️ ✓ ✎ 🗑️
8	VERDE	ROJA	TCP/143	→	allow IMAP	⬆️ ⬆️ ✓ ✎ 🗑️
9	VERDE	ROJA	TCP/995	→	allow POP3s	⬆️ ⬆️ ✓ ✎ 🗑️
10	VERDE	ROJA	TCP/993	→	allow IMAPs	⬆️ ⬆️ ✓ ✎ 🗑️
11	VERDE NARANJA	ROJA	TCP+UDP/53	→	allow DNS	⬆️ ⬆️ ✓ ✎ 🗑️
12	NARANJA	ROJA	TCP/80	→		⬆️ ✓ ✎ 🗑️

**35. La regla del servicio 8080 la creamos así, diciéndole que permite de origen Windows 7 (interna) con destino Windows xp (publica) salga por el puerto 8080, esto es para el hfs, ya que el utilizaba el puerto 80, pero ese puerto lo necesitamos para el servicio web de la dmz, entonces cambiamos el puerto para evitar conflictos.**

Sistema Estado Red Servicios Cortafuegos Proxy VPN Registros

Configuración del cortafuegos para el tráfico saliente

>> Reglas actuales

editor de reglas de salida del cortafuegos

<p>Origen</p> <p>Tipo * <span style="border: 1px solid gray; padding: 2px;">Red/IP</span></p> <p>Introduce los IPs/red (uno por línea)</p> <div style="border: 1px solid gray; padding: 2px; min-height: 40px;">192.168.30.30/24</div>	<p>Destino</p> <p>Tipo * <span style="border: 1px solid gray; padding: 2px;">Red/IP</span></p> <p>Introduce los IPs/red (uno por línea)</p> <div style="border: 1px solid gray; padding: 2px; min-height: 40px;">209.165.200.200/24</div>						
<p>Servicio/Puerto</p> <table style="width: 100%;"><tr><td>Servicio * <span style="border: 1px solid gray; padding: 2px;">&lt;Cualquiera&gt;</span></td><td>Protocolo * <span style="border: 1px solid gray; padding: 2px;">TCP</span></td><td>Puerto Destino (uno por Línea)</td></tr><tr><td colspan="3"><div style="border: 1px solid gray; padding: 2px; min-height: 20px;">8080</div></td></tr></table>		Servicio * <span style="border: 1px solid gray; padding: 2px;">&lt;Cualquiera&gt;</span>	Protocolo * <span style="border: 1px solid gray; padding: 2px;">TCP</span>	Puerto Destino (uno por Línea)	<div style="border: 1px solid gray; padding: 2px; min-height: 20px;">8080</div>		
Servicio * <span style="border: 1px solid gray; padding: 2px;">&lt;Cualquiera&gt;</span>	Protocolo * <span style="border: 1px solid gray; padding: 2px;">TCP</span>	Puerto Destino (uno por Línea)					
<div style="border: 1px solid gray; padding: 2px; min-height: 20px;">8080</div>							
<p>Política *</p> <table style="width: 100%;"><tr><td>Acción <span style="border: 1px solid gray; padding: 2px;">PERMITIR</span></td><td>Observación <span style="border: 1px solid gray; padding: 2px;">hfs</span></td><td>Posición * <span style="border: 1px solid gray; padding: 2px;">Primero</span></td></tr><tr><td><input checked="" type="checkbox"/> Activado</td><td colspan="2"><input type="checkbox"/> Registro de todos los Paquetes Aceptados</td></tr></table>		Acción <span style="border: 1px solid gray; padding: 2px;">PERMITIR</span>	Observación <span style="border: 1px solid gray; padding: 2px;">hfs</span>	Posición * <span style="border: 1px solid gray; padding: 2px;">Primero</span>	<input checked="" type="checkbox"/> Activado	<input type="checkbox"/> Registro de todos los Paquetes Aceptados	
Acción <span style="border: 1px solid gray; padding: 2px;">PERMITIR</span>	Observación <span style="border: 1px solid gray; padding: 2px;">hfs</span>	Posición * <span style="border: 1px solid gray; padding: 2px;">Primero</span>					
<input checked="" type="checkbox"/> Activado	<input type="checkbox"/> Registro de todos los Paquetes Aceptados						
<p><span>Actualizar regla</span> o <span>Cancelar</span></p>							

**36. Nos dirigimos a tráfico inter-zona, todas las reglas que se ven vienen por defecto, la única que creamos fue la política denegada, diciéndole que de origen naranja (dmz), con destino a la verde, deniegue el ping.**

## ENDIAN FIREWALL

The screenshot shows the 'Configuración del cortafuegos Inter-Zona' page. On the left, there is a navigation menu with options like 'Re-envío de puertos / NAT', 'Tráfico de salida', 'Tráfico Inter-Zona', 'Tráfico VPN', 'Acceso al sistema', and 'Firewall Diagrams'. The main content area is titled 'Reglas actuales' and contains a table of active rules. A link 'Agregar una nueva regla de cortafuegos inter-zona' is visible above the table. The table has columns for '#', 'Origen', 'Destino', 'Servicio', 'Política', 'Observación', and 'Acciones'. There are four rules listed, with the first three having a green arrow icon and the fourth having a red arrow icon. Below the table is a legend for the status icons and a 'Guardar' button.

#	Origen	Destino	Servicio	Política	Observación	Acciones
1	VERDE	NARANJA	TCP/80	→		↓ ↑ ✓ ✎ 🗑
2	VERDE	NARANJA	ICMP/8 ICMP/30	→		↓ ↑ ✓ ✎ 🗑
3	VERDE NARANJA	209.165.200.0/24	ICMP/8 ICMP/30	↔		↓ ↑ ✓ ✎ 🗑
4	NARANJA	VERDE	ICMP/8 ICMP/30	→		↓ ↑ ✓ ✎ 🗑

37. Así fue como se creó la regla.

The screenshot shows the 'Editar regla de zona del cortafuegos' page. It contains several form fields for configuring a rule. The 'Origen' and 'Destino' sections have dropdown menus for 'Tipo' and lists of interfaces. The 'Servicio/Puerto' section has dropdowns for 'Servicio' and 'Protocolo', and a text input for 'Puerto Destino'. The 'Política' section has a dropdown for 'Acción' and a checkbox for 'Activado'. There are also buttons for 'Actualizar Regla' and 'Cancelar'.

38. Nos dirigimos a las máquinas para rectificar si se ven o no por medio de un ping; vemos que Windows 7 da ping a la pública.

```
C:\Users\nata>ping 209.165.200.200
Haciendo ping a 209.165.200.200 con 32 bytes de datos:
Respuesta desde 209.165.200.200: bytes=32 tiempo<1m TTL=127
Respuesta desde 209.165.200.200: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 209.165.200.200:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Users\nata>
```



**39. Probamos ping hacia la dmz (zona naranja).**

```
C:\Users\nata>ping 192.168.20.2

Haciendo ping a 192.168.20.2 con 32 bytes de datos:
Respuesta desde 192.168.20.2: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.20.2: bytes=32 tiempo<1m TTL=63
Respuesta desde 192.168.20.2: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 192.168.20.2:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (<0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
```

**40. Nos situamos en Windows xp y damos ping a la dmz y si lo ve.**

```
> Símbolo del sistema
Respuesta desde 209.165.200.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 209.165.200.200: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 209.165.200.200:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (<0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Documents and Settings\Administrador>ping 192.168.20.2

Haciendo ping a 192.168.20.2 con 32 bytes de datos:
Respuesta desde 192.168.20.2: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.20.2: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 192.168.20.2:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (<0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 2ms, Media = 1ms
Control-C
^C
C:\Documents and Settings\Administrador>
```

**41. Ping de la roja a la verde falla, por las reglas ejecutadas.**

```
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

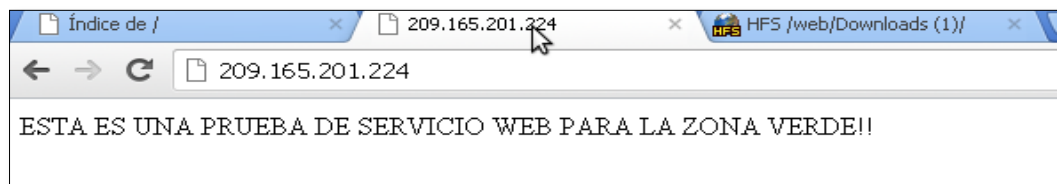
Estadísticas de ping para 192.168.30.30:
    Paquetes: enviados = 2, recibidos = 0, perdidos = 2
    (<100% perdidos),
```

**42. De la dmz a la inside no debe entrar, solo brinda servicios.**

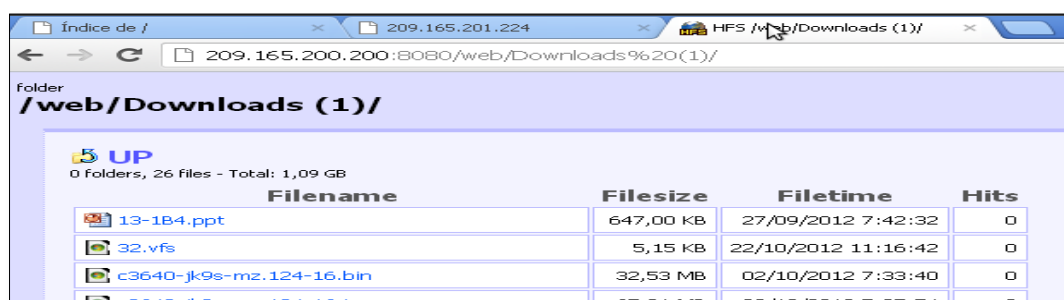
```
root@localhost:~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
[root@localhost Escritorio]# ping 192.168.30.30
PING 192.168.30.30 (192.168.30.30) 56(84) bytes of data.
From 192.168.20.2 icmp_seq=2 Destination Host Unreachable
From 192.168.20.2 icmp_seq=3 Destination Host Unreachable
From 192.168.20.2 icmp_seq=4 Destination Host Unreachable
^C
--- 192.168.30.30 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4667ms
pipe 3
[root@localhost Escritorio]#
```

**43. En Windows xp que es la outside, no dirigimos a el explorador y como url escribimos la ip publica con que la dmz debe ser vista por la outside, los servicios ftp y http (web).**

## ENDIAN FIREWALL



44. Y claro, tenemos el servicio hfs, por el puerto 8080 en la outside.



45. Ahora, nos dirigimos a la Windows 7 (zona verde), y entramos a los servicios de la dmz, además entramos al servicio HFS de la outside (zona roja).

