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



1. Instalando endian firewall.

Elegimos el idioma-ok.

EFW 2.4 (Community Edition) - Protect yourself
Language selection
Select the language you wish to use for the EFW.
Deutsch English Italiano
L 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.



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.





6. Ahora debemos darle la IP al endian.

Enter the IP address information for the GREEN interface.
IP address: Network mask: 255.255.0
0k Cancel

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.

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: _	<pre>Management URL: https://192.168.30.1:10443 Green IP : 192.168.30.1/None Ø) Shell 1) Reboot 2) Change Root Password 3) Change Admin Password 4) Restore Factory Defaults Choice: </pre>	Release: Endian	Firewall	Community	release	2.4.0	
<pre>Ø) Shell 1) Reboot 2) Change Root Password 3) Change Admin Password 4) Restore Factory Defaults Choice:</pre>	0) Shell 1) Reboot 2) Change Root Password 3) Change Admin Password 4) Restore Factory Defaults Choice: _	Management URL: Green IP :	https:/// 192.168.3	192.168.30 30.1∕None	.1:10443		
Choice: _	Choice: _	0) Shell 1) Reboot 2) Change Root I 3) Change Admin 4) Restore Facto	Password Password ory Defaul	lts			
*		Choice: _					
						k	

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.

rootOf ire	wall:~ # ifconfig
brØ	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 butes:123527 (120.6 KiB) TX butes: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.

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.

Propiedades: Protocolo de Internet versió	n 4 (TCP/IPv4)			
General				
Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.				
Obtener una dirección IP automática	nente			
O Usar la siguiente dirección IP:				
Dirección IP:	192 . 168 . 30 . 30			
Máscara de subred:	255 . 255 . 255 . 0			
Puerta de enlace predeterminada:	192.168.30.1			
Obtener la dirección del servidor DNS	automáticamente			
 Usar las siguientes direcciones de ser 	vidor DNS:			
Servidor DNS preferido:				
Servidor DNS alternativo:				
Validar configuración al salir	Opciones avanzadas			
	Aceptar Cancelar			

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

крs ://192	168.30.1:10443
	El certificado de seguridad del sitio no es de confianza.
	Has intentado acceder a 192.168.30.1 , pero el servidor ha presentado un certificado emitido por una entidad que el sistema operativo del ordenador no tiene registrada como entidad de confianza. Este problema se puede deber a que el servidor haya generado sus propias credenciales de seguridad (en las que Google Chrome no puede confiar para confirmar la autenticidad del sitio) o a que una persona esté intentando interceptar tus comunicaciones.
	No deberías continuar, sobre todo si no has recibido nunca esta advertencia para este sitio. Continuar de todos medos Volver a seguridad Más información

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 ">>>".



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

_			? ¹ Help	A Logout
endian firewall community				
>> Welcome to Endian Firewal	I			
	Welco	me to Endian Firewall		
	Please select your language:	Spanish (Español)	•	
	Timezone:	America/Bogota	•	
		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
	Endian Firewall Com	munity release 2.4.0 (c) 2004-2009 Endia	in	

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

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
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 softwareto 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
<pre>&gt;&gt;&gt;</pre>

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

	? Ayuda	Cerrar sesión
endian firewall		
Commonly		
>> Importar respaldo		
¿Desea restaurar un respaldo? No 💌		
Cancela >>>		
Endian Firewall Community release 2.4.0 (c) 2004-20	09 Endian	

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

		Ayuda	Cerrar sesión
endian firewall			
communir	У		
>> Cambiar la Contraseñ	ia por Defecto		
	Contraseña (admin) de la interfaz web	Contraseña (root) SSH	
	Contraseña *	Contraseña *	
	Confirmar Contraseña *	Confirmar Contraseña *	
	Cancelar	>>>	
	Endian Firewall Community rel	ease 2.4.0 (c) 2004-2009 Endian	

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

endian firewall community	
>> Ayudante de configuración de red	
Paso 1/8: Seleccionar el Tipo de Interface ROJA	
ROJA: Conección a Internet (WAN), no Confiable	Información del Hardware
ETHERNET ESTATICO	Numero de Interfaces 3
© ETERNET POR DHCP	
© PPPoE	
C ADSL por (USB o PCI)	
© RDSI	
Modem ANALOGICO/UMTS	
PUERTA DE ACCESO	
Cancelar >>>	

19. Elegimos la interfaz a configurar clic >>>

O	endıan firewall. COMMUNITY
	>> Ayudante de configuración de red
	Paso 2/8: Seleccione la Zonas de Red
	NARANJA: Servidores en Segmento de Red Accesibles desde Internet (DMZ)
	AZUL: Segmento de Red Para Clientes Inhalámbricos (WIFI)
	© NINGUNO
	© AZUL
	<<< Cancelar >>>

20. Le damos el Gateway de la zona verde "inside"

	irewall <b>NUNITY</b>								
	Sistema	Estado	Red	Servicios (	ortafuegos	Proxy	VPN	Registros	
	Configura	ción de	Red						
hboard	>> Ayudar	te de confi	guración de reo	1					
figuración de Red	Dana 2/2: Da	forencian	do rod						
ficaciones de eventos	- Paso 3/8: Pr	ererencias	de red						
traseñas	VERDE (Rec	I Interna (L	AN) de Confian	za):					
ceso SSH	Disconition		400 400 00 4				04 055 05	10 000 0	
stes del GUI	- Dirección iP		192.100.30.1		Mascara de R	ed.	/24 - 200.20	5.255.0	
ia de respaldo	Añadir Dire	ciones Ad	icionales (una l	P/Mascara o IP/CI	OR por linea) :				
gar									
réditos:									
				11					
	Interfaces:		N						
	Puer	o Vinculo	کا Descripción	MAC	Dispositivo				
	☑ 1	1	Intel ?	08:00:27:72:4e:4	9 eth0				
		. 4	1-1-1-2	00-00-07-bb-45-	-				
	2	~	intel <u>r</u>	08:00:27:bb:d5:3	os etni				
	3	<b>~</b>	Intel ?	08:00:27:a9:fa:a	3 eth2				

NARANJA (Servidores en Segmento de Red Accesibles desde Internet (DMZ)):										
Direc	ción IP:	1	192.168.20.1		Máscara de R	ed:	/24 - 255.25	55.255.0	-	
Añad	dir Direcc	iones Adi	cionales (una	IP/Mascara o IP/CIDR	t por linea) :					
Inter	faces:									
	Puerto	Vinculo	Descripcio	on MAC	Dispositivo					
	1	<b>~</b>	Intel ?	08:00:27:72:4e:49	eth0					
	2	<b>~</b>	Intel ?	08:00:27:bb:d5:33	eth1					
	з	~	Intel ?	08:00:27:a9:fa:a3	eth2					
Nom An fit	bre del rión:	ł	firewall							
Nom	bre del D	ominio:	ocaldomain							
	<	Cancelar	>>>							

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

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

ROJ	A (Coned	ción a Inte	rnet (WAN), no	Confiable):		
Direc	ción IP:	209.1	209.165.200.1 Máscara de Red:			
Añad	dir Direco	iones Adio	ionales (una IP	/Mascara o IP/CIDF	R por linea) :	
Inter	faces:					
	Puerto	Vinculo	Descripción	MAC	Dispositivo	
	1	~	Intel ?	08:00:27:72:4e:49	eth0	
	2	~	Intel ?	08:00:27:bb:d5:33	eth1	
۲	3	~	Intel ?	08:00:27:a9:fa:a3	eth2	
Puer	ta de enla	ace predet	erminada:	209.1	65.200.1	
мти: 🖜						
"Spoof" la dirección MAC con:						
Opo						
• Б	ste camp	o puede a	uedar en blanc	0		
_				-		

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

Configuración de Red							
>> Ayu	dante de configuració	ón de red					
Paso 5/8	Configurar DNS						
Configur	ación Manual DNS:						
DNS 1:	209.165.200.1	]					
DNS 2:	209.165.200.1	1					
	Cancelar	>>>					

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

configuración de Red							
>> Ayudante de configuración de	e red						
Paso 6/8: Configure default admin mail							
Admin email address:  brendatovar@misen							
Sender email address:							
Dirección del host smarthost: ●							
Este campo puede quedar en l	blanco						
Cancelar >	~>>						

# 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.

Left Editando Auto eth3 のよう になった。	ĸ
Nombre de la conexión: Auto eth3	]
☑ Conectar <u>a</u> utomáticamente	
Cableado Seguridad 802.1x Ajustes de IPv4 Ajustes de IPv6	
Método: Manual	
Direcciones	
Dirección Máscara de red Puerta de enlace <u>A</u> ñadir	
192.168.20.2 255.255.255.0 192.168.20.1	
Servidores DNS:	
Dominios de bú <u>s</u> queda:	
ID del cliente D <u>H</u> CP:	
☑ Requiere dirección IPv4 para que esta conexión se complete	
Boutes	
☑ Disponible para todos los usuarios	]

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



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

← → ✓ 🔁 区 🚔 🖳 ftp://192.168.20.2/	숫 🗸 Google 🔍
🛅 Más visitados 🗸 💿 Centos 💿 Wiki 💿 Documentation 💿 Forums	
Number 2012 Indice de ftp://192.168.20.2/	ф <b>~</b>
Índice de ftp://192.168.20.2/	
🕈 Subir al directorio superior.	
Nombre	Tamaño Última modificación 22/06/12 07:54:00
🔶 🔶 🛛 😂 🕜 🕋 💽 http://192.168.2	20.2/
🗑 Más visitados 🗸 💿 Centos 💿 Wiki 💿 Docum	entation 🐻 Forums

ESTA ES UNA PRUEBA DE SERVICIO HTML PARA LA ZONA VERDE!!

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

C & https://192.1	. <b>68.30.1</b> :10443/cgi-bi	n/dnat.cgi					
	irewall. <b>NUNITY</b>				<b>21</b> Ayuda	Cerrar sesión	
	Sistema Estado	Red Ser	vicios C	ortafuegos P	roxy VPN	Registros	
	Port forwarding /	Destination N	IAT				
Re-envio de puertos / NAT	Port forwarding	J / Destination N/	AT NAT fue	nte Incoming route	ed traffic		
Trafico de salida							
Tráfico Inter-Zona							
Tráfico VPN							
Acceso al sistema							
Firewall Diagrams							
	>> Reglas actuales						
	Add a new Port fo	rwarding / Destina	tion NAT rule				
	# Incoming IP	Servicio	Política	Translate to		Observación	Acciones
	1 209.165.201.224	TC 21	- <del>53</del>	192.168.20.2 : 21		traduccion out ftp	♦ 🗹 🛈 🦉 🕯
	ALLOW with IPS f	rom:		<cualquiera></cualquiera>			Ø 1
	2 209.165.201.224	TCP/80	<b>%</b>	192.168.20.2 : 80		traduccion out web	+ 🗹 O 🦉 🕽
	ALLOW with IPS f	rom:		<cualquiera></cualquiera>			Ø 5
	Leyenda: 📝 Habilita	ado (click para des	habilitar) 🗌	Deshabilitado (click	k para habilitar)	🥜 Editar 📑 Eliminar	

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 fir	ewall. Unity
	Sistema Estado Red Servicios <mark>Cortafuegos</mark> Proxy VPN Registros
	Port forwarding / Destination NAT
Re-envío de puertos / NAT	Port forwarding / Destination NAT NAT fuente Incoming routed traffic
Trafico de salida	
Tráfico Inter-Zona	>> Keglas actuales
Tráfico VPN	Desk forwarding / Deskinsking MAT Bule Fuller
Acceso al sistema	Port forwarding / Destination NAT Rule Editor Simple Mode   Advanced Mode
The mail olagians	Incoming IP Tipo * Red/IP/Rango Introduce los IPs/red (uno por línea) 209.165.201.224 Protocolo * TCP I Incoming Service/Port Servicio * Incoming port/range (one per líne, e.g. 80, 80.88) Introduce los IPs/red (uno por línea)
	Translate to *           Insertar IP         Port/Range (e.g. 80, 80:88)         NAT
	192.168.20.2 21 NAT 💌
	Activado Registro Observación traduccion out ftp     Posición * Primero
	Actualizar Regla o Cancelar * 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).

	ewall
	Sistema Estado Red Servicios Cortafuegos Proxy VPN Registros
	Port forwarding / Destination NAT
Re-envío de puertos / NAT	Port forwarding / Destination NAT NAT fuente Incoming routed traffic
Trafico de salida	
Tráfico Inter-Zona	>> Reglas actuales
Tráfico VPN	
Acceso al sistema	Port forwarding / Destination NAT Rule Editor Simple Mode   Advanced Mode
Firewall Diagrams	Incoming IP Tipo * Red/IP/Rango Tipo * Red/IP/Rango Introduce los IPs/red (uno por línea) U09.165.201.224 Introduce los IPs/red (uno por línea) TCP
	Translate to *         Insertar IP       Port/Range (e.g. 80, 80:88)       NAT         192.168.20.2       80       NAT         IV Activado       Registro       Observación traduccion out web       Posición * Después de la Regla #1 •         Actualizar Regia       o Cancelar       * Este campo es obligatorio.

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

endian firewall community									
	Sistema	Estado	Red	Servicios	Cortafuegos	Proxy	VPN	Registros	
	Incoming	firewall c	onfigura	ation					
Re-envio de puertos / NAT	» Port fo	orwarding / D	estination I	NAT NAT fuen	te Incoming r	outed traffic			
Trafico de salida									
Tráfico Inter-Zona	>> Reglas actuales								
Tráfico VPN	Agregar una pueva regla del cortafuegos								
Acceso al sistema									
Firewall Diagrams	# Orige	n		Destino		Servicio	Política	Observación	Acciones
	1 <cualq< td=""><td>uiera&gt;</td><td></td><td>NARANJA</td><td></td><td><cualquiera></cualquiera></td><td>-<b>F</b></td><td></td><td>🗹 🥒 🗊</td></cualq<>	uiera>		NARANJA		<cualquiera></cualquiera>	- <b>F</b>		🗹 🥒 🗊
	Leyenda Mostrar la	I Habilitad	do (click pa I sistema	ara deshabilitar) a >> &	Deshabilitad	o (click para hai	bilitar) 🥜	Editar 📅 Eliminar	

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

endian fil comm	rewall
	Sistema Estado Red Servicios Cortafuegos Proxy VPN Registros
	Incoming firewall configuration
Re-envío de puertos / NAT	Port forwarding / Destination NAT NAT fuente Incoming routed traffic
Tráfico Inter-Zona	>> Reglas actuales
Tráfico VPN Acceso al sistema	Incoming Routed Traffic Firewall Rule Editor
Firewall Diagrams	Origen     Destino       Tipo *     <       Tipo *        Zonas        Esta regla se aplicará a toda la ROJA     Select zones (hold CTRL for multiselect)       VERDE        NARANJA        Servicio/Puerto        Servicio *     Protocolo *        Puerto Destino (uno por Línea)
	Política * Acción ALLOW with IPS Observación Posición * Primero  Activado Registro de todos los Paquetes Aceptados Actualizar regia o Cancelar * Este campo es obligatorio.

# 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.

		Las reglas de co	ortafuego fueron apl	licadas exit	osamente	
>>	Reglas actuales					
٢	Agregar una nueva regla d	lel 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	⇒		
з	VERDE	ROJA	TCP/80	- <b>5</b>	allow HTTP	
4	VERDE AZUL	ROJA	TCP/443	<del>-</del> 5 <del>3</del>	allow HTTPS	+ + 🗹 🥒 🖻
5	VERDE	ROJA	TCP/21	- <del>5</del> ->>	allow FTP	
6	VERDE	ROJA	TCP/25	- <b>5</b>	allow SMTP	
7	VERDE	ROJA	TCP/110	- <b>5</b>	allow POP	
8	VERDE	ROJA	TCP/143	- <b>5</b>	allow IMAP	
9	VERDE	ROJA	TCP/995	- <b>5</b> ->	allow POP3s	
10	VERDE	ROJA	TCP/993	- <b>5</b>	allow IMAPs	
11	VERDE NARANJA	ROJA	TCP+UDP/53	<del>-</del> /34	allow DNS	* * 🗹 🥒 😭
12	NARANJA	ROJA	TCP/80			A A A A A A A A A A A A A A A A A A A

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
	Configura	ación del	cortafue	egos para e	el tráfico salie	ente		
Re-envío de puertos / NAT	>> Regla	as actuales						
Trafico de salida								
Tráfico Inter-Zona	editor	de reglas de	salida de	l cortafuegos				
Tráfico VPN	Origen					Destino		
Acceso al sistema	Tino *	Ded//D				Tipo * Ded/	•	1
Firewall Diagrams	ripo -	Red/IP	•			ripo - Redri	r 💌	
	Introduc	e los IPs/red (	uno por líne	ea)		Introduce los I	Ps/red (uno	por línea)
	Servici Servici <cual< td=""><td>io/Puerto io* Iquiera&gt;</td><td>Protoc</td><td>colo * I</td><td>Puerto Destino (un 8080</td><td>o por Línea)</td><td>ž</td><td></td></cual<>	io/Puerto io* Iquiera>	Protoc	colo * I	Puerto Destino (un 8080	o por Línea)	ž	
	Política	a *						
	Acción		-	Observación				Posición *
	PERM			nis				Primero
	✓ Ac	tivado		Registro d	le todos los Paque	tes Aceptados	6	
	Actua	alizar regla 🛛 o	Cancelar					

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 f	nunity							
	Sistema Esta	do Red	Servicios	Cortafuegos	Proxy	VPN	Registros	
	Configuración	del cortafi	iegos Inter-2	Zona				
Re-envío de puertos / NAT	» Reglas actua	es						
Trafico de salida								
Fráfico Inter-Zona	Agregar una r	ueva regia de	cortatuegos intel	-zona				
Tráfico VPN	# Origen		Destino		Servicio	Política	Observación	Acciones
Acceso al sistema	1 VERDE		NARANJA		TCP/80	<b>a</b>		🌵 🗹 🥔 👕
Firewall Diagrams	2 VERDE		NARANJA		ICMP/8 ICMP/30	<b>+</b>		1 4 🖉 🥜 🕃
	3 VERDE NARANJA		209.165.200.	0/24	ICMP/8 ICMP/30	<del>-</del> ?#		1
	4 NARANJA		VERDE		ICMP/8 ICMP/30	⇒ <b>i</b>		🕈 🗹 🖉 🖻
	Leyenda: 📝 H Mostrar las regl » Configuracion	abilitado (click as de los ser es de Inter-Zo	para deshabilitar vicios del siste na del Cortafueg	) 🗌 Deshabilita ema >>	do (click para l	habilitar) 🎸	🖉 Editar 🥤 Eliminar	
	Habilitar corta	uegos Inter	-Zona »					
	Guardar		5 65 ING -2010					

#### 37. Así fue como se creó la regla.

endian fi	rewall
	Sistema Estado Red Servicios <mark>Cortafuegos</mark> Proxy VPN Registros
	Configuración del cortafuegos Inter-Zona
Re-envío de puertos / NAT	>> Reglas actuales
Trafico de salida	
Tráfico Inter-Zona	Editar regla de zona del cortafuegos
Tráfico VPN	Origan
Acceso al sistema	
Firewall Diagrams	
	VERUE A NARANJA NARANJA Interfaz 1 (Zona: VERDE) Interfaz 2 (Zona: NARANJA)
	Servicio/Puerto       Servicio * <cualquiera>       ICMP         8</cualquiera>
	Política Acción * Observación Posición * DENEGAR DENEGAR Después de la Regla #3 Activado Registro de todos los Paquetes Aceptados
	Actualizar Regla o Cancelar *Este campo es obligatorio.

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.



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

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



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.

 Image: contract of the second seco

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).

$\leftarrow \rightarrow$	C 🗋 ftp://20	09.165.201.22	4 🔓		
Índi	ce de /				
Nombre	Tamaño	Fecha de 1 22/06	<b>nodificaci</b> /12 07:54:	<b>ón</b> 00	
<ul> <li>É Índice de /</li> <li>← → C</li> </ul>	× 209.165.201.224	9.165.201.224	× 讨 HFS /web	/Downloads (1)/	×
ESTA ES UNA	A PRUEBA DE SERVI	ICIO WEB PARA L	a zona veri	DEII	

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

C	) Índice de /	× 🔨 🗅 209.165.201.224	× 🖌 📾 H	HFS /whyb/Downloads (1)/	×	5
←	⇒ C	209.165.200.200:8080/web/Downlo	ads%20(1)/			
fold /v	veb/D¢	ownloads (1)/				
	5 UP 0 folders,	26 files - Total: 1,09 GB				
		Filename	Filesize	Filetime	Hits	
	👫 13-	LB4.ppt	647,00 KB	27/09/2012 7:42:32	0	
	<b>0</b> 32.v	fs	5,15 KB	22/10/2012 11:16:42	0	
	💽 c36	40-jk9s-mz.124-16.bin	32,53 MB	02/10/2012 7:33:40	0	
	<b>IR</b> -26	10. ik00. mp. 104-16 impage	65 01 MD	02/10/2012 7:25:54		

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).

		.168.20.2	N ×	🖞 India	ce de /
← → C 🗋	192.168.20.2		65		
ESTA ES UNA	PRUEBA DE SE	ERVICI	O WEB PARA	A LA	ZONA VERDE!!
🔾 Endian Fire	wall - Zona de c	168.20	192.168.20.2		*7 🖿
Índice	e de /				
Nombre pub/	Tamaño	Fe	cha de m 22/06	3/12	ficación 07:54:00
😜 Endian Firewall - Zona de	c × \ 🙀 192.168.20.2	× /[]]	Indice de /	×/ 📾	HFS /web Oownloads (1)/ ×
<ul> <li>Endian Firewall - Zona de</li> <li>         → C          <ul> <li>209.165</li> </ul> </li> </ul>	c× \	× \ل۲ ا loads%20(1)	(ndice de /	×/ 📾	HFS /wet Sownloads (1)/ ×
<ul> <li>➡ Endian Firewall - Zona de</li> <li>➡ ➡ C □ 209.165</li> <li>older</li> <li>/web/Downloads</li> </ul>	<pre>&lt; \ 192.168.20.2 .200.200:8080/web/Downl s (1)/</pre>	× \[] loads%20(1)	índice de / /		HFS /wett꽃ownloads (1)/ ×
Endian Firewall - Zona de E -> C 2 209.165 older /web/Downloads 5 UP 0 folders, 26 files - Total: 1	<pre>&lt; \</pre>	× \[] loads%20(1)	Indice de / /	×/ 📾	HFS /wetty ownloads (1)/ ×
C Endian Firewall - Zona de C 209.165 older / web/Downloads UP 0 folders, 26 files - Total: 1 Fi	<pre>c× 192.168.20.2 .200.200:8080/web/Downl s (1)/ .09 GB ilename</pre>	× U1 loads%20(1) Filesize	findice de / / Filetime	× ma	HFS /welt Yownloads (1)/ ×
C Endian Firewall - Zona de C → C ○ 209.165 older / web/Download: UP 0 folders, 26 files - Total: 1 Fi I 3-1B4.ppt	<pre>c× 192.168.20.2 .200.200.8080/web/Downl s (1)/ .09 G8 ilename</pre>	× ([]] loads%20(1) Filesize 647,00 KB	Filetime 27/09/2012 7:42:32	× maa Hits	HFS /wett Yownloads (1)/ ×
C Endian Firewall - Zona de C → C 209.165 Colder /web/Download: 5 UP 0 folders, 26 files - Total: 1 Fi 13-1B4.ppt 0 32.vfs	<pre>cx im 192.168.20.2 .200.200.8080/web/Downl s (1)/ .09 GB ilename</pre>	× ([]] loads%20(1) Filesize 647,00 KB 5,15 KB	Filetime 27/09/2012 7:42:32 22/10/2012 11:16:42	× the second sec	HFS /wett Yownloads (1)/ ×
C Endian Firewall - Zona de ← → C 209.165 folder /web/Download: Ø Folders, 26 files - Total: 1 File: 13-184.ppt ③ 32.vfs ③ c3640-jk9s-mz.12	<pre>cx \mathbf{iii} 192:168:20.2 200.200:8080/web/Downl s (1)/</pre>	× (С) loads%20(1) Filesize 647,00 КВ 5,15 КВ 32,53 MB	Filetime 27/09/2012 7:42:32 22/10/2012 11:16:42 02/10/2012 7:33:40	Hits 0 0 0	HFS /wett Yownloads (1)/ ×