Cortafuegos con Windows 2000 o XP

Por José Mariscal Prieto i72maprj@uco.es Página Web Todos los derechos reservados, este texto esta registrado.

1. Cómo montar un cortafuegos sin software adicional

Windows 2000, y Windows XP tienen la posibilidad de crear reglas de filtrado para montar un cortafuegos sin la necesidad de instalar un software adicional, así controlamos que instalamos. También aquellos usuarios que solo tengan un PC, si tienen varios en Red pueden que tengan problemas si no se configura correctamente. Esto va dirigido a los usuarios mas noveles, los administradores avanzados sabrán como modificar las directivas de seguridad, aunque seguramente usarán algún cortafuegos que es mucho mejor que esto. Además dispone de un asistente para agregar reglas de filtrado, el único inconveniente es que hay que bloquear puerto por puerto los que queramos bloquear. Para ello nos vamos al Panel de Control, y dentro de este Herramientas Administrativas, donde seleccionamos **Directiva de Seguridad local**.



Figura 1: En la imagen Herramientas Administrativas, dentro del Panel de Control

Se nos abrirán las Directivas de Seguridad, entre estas la Directiva de Seguridad IP. Seleccionamos el icono de **Directivas de seguridad IP en la Máquina local**, y en la parte derecha hacemos click con el botón derecho, y le damos a **Crear directiva de seguridad IP**

📑 Configuración de seguridad local				_ 🗆 🗵
📙 Acción Ver 📙 🖨 🔁 🖬 🔂	😫 🛅 ≟			
Árbol	Nombre 🔺	Descripción	Directiva asignada	
Configuración de seguridad Configuración de seguridad Directivas de cuenta Configuración de seguridad Directivas de claves públicas Configuración de seguridad IP en Máquina local	 Cliente (sólo responder) Servidor (Pedir seguri Servidor seguro (requ Crear directiva de se Administrar listas de Todas las tareas 	Comunicarse normalmente (Para todo el tráfico IP, siem Para todo el tráfico IP, siem guridad IP filtros IP y acciones de filtrado	No No No	
	Actualizar Exportar lista Ver Organizar iconos Alinear iconos Ayuda			
	nes de filtrado disponibles			

Figura 2: Las Directivas de Seguridad IP permiten crear nuevas opciones de Filtrado IP

Lo que vamos a hacer es crear un cortafuegos siguiendo los siguientes pasos:

- 1. Crear una Directiva de seguridad. Cortafuegos
- 2. Crear una Lista de Filtros. No Dejar
- 3. Crear una acción de Filtrado, aplicable a la lista de filtros. Filtrado Bloquear
- 4. Activar la Directiva de seguridad.

Ruego encarecidamente que si tu equipo esta dentro de una red corporativa, avisa a tu Administrador de Red ya que podrías generar conflictos en tu red y no podrían acceder a tus datos, según el diseño del sistema.

Windows posee un asistente que usaremos para crear una nueva directiva y bloquear un puerto de ejemplo. Este asistente se inicia de manera automática. Lo que haremos sera crear primero una directiva y luego ampliar esa directiva, con los puertos que queramos bloquear.



Figura 3: El asistente permite crear nuevas opciones de filtrado de manera sencilla.

Lo único que tendremos que decirle es el nombre de la directiva. Esta es la directiva que mencionamos al principio, es la que va a almacenar la lista de filtros, y la acción que hacer.

Podemos asignarle una descripción: Esta directiva, lo que va a hacer es bloquear los puertos mas proclives de ser atacados.

tent	e para directivas de seguridad IP	2
Nom F	bre de la directiva de seguridad IP ^P óngale un nombre a la directiva de seguridad y, si lo desea, escriba también una preve descripción.	
<u>1</u>	<u>√</u> ombre:	
	Cortafuegos	
Ξ	2escripción:	
Γ		A
		-
	Zátrás Siguiente D	ancelar
		ancolar

Figura 4: Le asignamos un nombre a la Directiva, por ejemplo Cortafuegos.

Los filtros podemos englobarlos, y ser utilizados dentro de una misma directiva. Podemos tener varias directivas pero sólo *una estará activa* en nuestro sistema, es decir no podremos utilizar varias directivas a la vez. Se explicará como activar una directiva en el último paso.

Eligiremos el método predeterminado, ya que no necesitaremos otra normativa mas avanzada.

do de autenticación de la regla d ara agregar varios métodos de autentica espuesta predeterminada una vez se haj	e respuesta predetermi ación múltiple, modifique la r ya completado el asistente.	inada regla de
stablezca el método de autenticación in	icial para esta regla de segu	uridad:
Valor predeterminado de Windows 20	00 (protocolo Kerberos V5)	
Use un <u>c</u> ertificado de esta autoridad o	de certificados (CA):	
		E <u>x</u> aminar.
-		

Figura 5: Windows soporta varios métodos de Autenticación, utilizaremos el predeterminado.

Seguramente nos saldrá una advertencia, nuestro equipo no está dentro de un Dominio, más si solo tenemos nuestro equipo, le damos a SI.

Ya disponemos de una directiva de seguridad IP, modificando sus propiedades podremos ampliar esta política para que bloquee los puertos que estimemos necesarios.

Asistente para directivas de :	seguridad IP	? ×
	 Finalización del Asistente para directivas de seguridad IP Ha completado satisfactoriamente la especificación de las propiedades de su directiva de seguridad IP. Para modificar ahora su directiva de seguridad, seleccione la casilla de verificación Modificar propiedades, y luego haga clic en Finalizar. Modificar las propiedades 	
	Para cerrar este asistente, haga clic en Finalizar.	
	< <u>A</u> trás Finalizar Cancela	JI

Figura 6: Tenemos la directiva de seguridad creada, solo hay que modificar sus propiedades.

Para bloquear los puertos que queramos crearemos filtros, en el ejemplo crearemos solo uno, y luego al final se dará un resumen sobre los puertos que debemos bloquear y que podrían poner en un aprieto a nuestro sistema.

Si todo ha ido bien, ya tenemos nuestra directiva de seguridad IP creada. Podemos eliminar la regla de Dinámico. Porque lo que queremos hacer es crea nuevos Filtros que nos permitan bloquear los puertos y protocolos que no queremos que accedan a nuestro ordenador.

piedades de Cortafu	legos		?
eglas General E Reglas de s	eguridad para establecer c	omunicación con e	quipos
Reglas de seguridad IP	: A : Z - d - Chur d -	Martin	Conformatión
Lista de filtros IP	Acción de rittrado		Configuración .
Agregar Mo	dificar Quitar	1 🖬 🗤	•
			nte para agregar
		Aceptar	

Figura 7: Esta es nuestra ventana, ya tenemos la directiva creada

Especificaremos que no utilice tunel, un tunel une dos redes separadas por Internet o otra red que haya de por medio, mediante un protocolo de seguridad como IPSec.

sistente p	para re	glas i	le se	guri	dad										? ×
Punto I El e des de s	f inal de extremo f tino del l segurida	l tún nal de ráfico d.	el I túne IP, co	lese mov	el equ viene	ipo c espe	on pro cifica	otoc do e	colo de en la lis	túne ta de	el más (e filtros	ercar IP de	io al las reg	glas	Ē
Un I (Inte entr	túnel IP9 ernet/intr e dos ec	iec pe anet) juipos	ermite con el	a los I nive	paqu I de s	etes :eguri	atravo idad o	e u	r una re ina con	ed pü iexió	ública c n priva	priva da y d	da irecta		
Esp	ecifique	el exti	emo d	lel tú	nel pa	ara la	regla	de	seguria	dad I	P:				
۲	Esta reg	la no i	especi	ifica (un túr	nel									
c	Elextrer	no del	túnel	se es	specif	ica m	nediar	te e	esta dir	ecci	ón IP:				
	0		0	1	0		0								
									< Atrá	s	Sig	uiente	>	Ca	ancelar
							1	_			28		105		

Figura 8: No especificaremos un tunel.

Si disponemos de una red interna, deberemos luego crear una regla que permita a la red Interna que tiene un rango de IPs poder acceder a nuestro equipo.



Figura 9: Por defecto pondremos Todas las conexiones de red.

Para Crear nuevos Filtros le damos a aceptar.

ente para reglas de se	guridad	
sta de filtros IP Seleccione la lista de fi seguridad.	tros IP para el tipo de tráfico IP al que s	e aplica la regla de
Si no hay un filtro IP en en Agregar para crear u	la siguiente lista que coincida con sus r ino nuevo.	necesidades, haga clic
Listas de filtros IP:		
Nombre	Descripción	Agr <u>eg</u> ar
		Modificar
		Quitar
2		
	7 Abrés 🔽	Siguianto X
	<u> </u>	

Figura 10: La lista de Filtros IP está vacia hay que crear nuevos.

Podemos tener varios filtros que engloben a varios puertos o bien, separandolos por protocolos. Sencillamente con esto podemos tener mejor organizada nuestros filtros. Pero por ejemplo en vez de no dejar, podíamos haberle puesto *No Dejar TCP* y meter todos los filtros de ese protocolo, y otro para el UDP.

Nombre:	1			
) escripcio	ón:			Agregar
				Modificar
			T	Quitar
Filtros:			🔽 Usar Asiste	nte para agregar
Distan	Descripción	Protocolo	Puerto de origen	Puerto de destin

Figura 11: Le ponemos un nombre a nuestro filtro, por ejemplo No Dejar.

Como he dicho es mejor separar los protocolos en diferentes filtros por el hecho de que se han de añadir uno por uno y puede ser algo tedioso

Aquí conviene tener unas nociones básicas de internet. Una dirección IP es un numero identificativo que tiene cualquier ordenador conectado a internet. Es lo que nos identifica en Internet, si bien una IP puede ser fija o variable, dependiendo de nuestra conexión o como lo tengamos contratado.

Asistente para filtros		? ×
Origen del tráfico IP Especifique la dirección de origen del tráfico	IP.	Ĩ
Dirección de origen: Cualquier dirección IP		
	< Atrás Siguier	nte > Cancelar

Figura 12: El origen Cualquier Direccion IP.

Para iniciar conexiones, una máquina es la que inicia la conexión, el origen. Expecificando cualquier dirección IP, estamos diciendo que puede ser cualquier ordenador de internet. En realidad especificamos la mascara 0.0.0.0 con esto se dice que puede ser cualquier ordenador.

El destino es el ordenador al cual va dirigida esa conexión. Este va a ser nuestro ordenador y la ip que tendra puede ser la nuestra, la que tenga nuestro ordenador.

Asistente para filtros			<u>?×</u>
Destino del tráfico IP Especifique la dirección de destino del tráfico l	IP.		Ē
Dirección de destino:			
Mi dirección IP		[
			12 22
	< Atrás	Siguiente >	Cancelar

Figura 13: El destino Mi Dirección IP.

Puede que tengamos varias Interfaces de red o varias direcciones IP, aunque no las sepamos se aplicará a todas las direcciones IP que posea nuestra maquina, excepto la loopback¹

¹Loopback o la IP 127.0.0.1, es la dirección que tienen todos los ordenadores con si mismos y sólo ellos mismos pueden acceder, se utiliza para pruebas.

El protocolo TCP es un protocolo a nivel de transporte, no comviene confundirlo con los de aplicación por ejemplo, pop, http, smtp... Los de aplicación vienen definidos por un puerto.

sistente para filtros	? ×
Tipo de protocolo IP Seleccione un tipo de protocolo IP. Si éste es compatible con puertos IP, deberá especificar también el puerto IP.	Ð
Seleccione un tipo de protocolo:	
Cualquiera 💌	
RDP BVD	
< Atrás Siguiente > C	ancelar

Figura 14: Protocolo TCP

Aqui algunos protocolos a nivel de aplicación que utilizan TCP y sus puertos:

Nombre	Explicación	Puerto
FTP	Transferencia de Ficheros	21
SMTP	Envio de correo	25
HTTP	Web, páginas web	80
POP	Recepción de correo	110
IRC	Chat	6667

Estos son algunos de los mas utilizados del protocolo de transporte TCP.

Este puerto es el que usa una aplicación, un servicio que permite el acceso a recursos o información de nuestro sistema. El puerto 137 lo utiliza windows para los nombres de NetBIOS, es un protocolo de aplicación ² utilizado por windows para cambiar ficheros. Piense que mientras mas bloquee un sistema mas difícil sera que puedan accederle, pero también piense que pierde desempeño en las labores que puede usted realizar.

sistente para filtros	? ×
Puerto de protocolo IP La mayoría de los protocolos de red IP se establecen con puertos IP conocidos.	đ
Establezca el puerto de protocolo IP:	
Desde este puerto:	
C A cualquier puerto	
A este puerto:	
137	
< Atrás Siguiente > 0	Cancelar

Figura 15: El puerto de Destino 137.

Puede que piense que puede tener un puerto activo y puede que no le soliciten información o aun asi que no puedan acceder, es una forma de pensar pero también existe la posibilidad de que se descubra un fallo que mandando una determinada petición cause el cuelge del sistema o el uso de todos sus recursos.

²Cada protocolo de aplicación tiene asignado un puerto, por ejemplo el 80 el web, o el 25 smtp (correo)

Ya tenemos el filtro creado, ahora debemos verificar las propiedades o agregar otro filtro adicional, por ejemplo agregando otro puerto el cual bloquear.



Figura 16: Verificamos las propiedades de nuestro filtro

Si bien esta creado, con esto no es sufuciente, debemos saber que hacer con estos filtros, en los siguientes pasos se explicará como crear politicas para estos tipos de filtros, es decir que vamos a hacer cuando nos llege una petición para esa conexión *aceptarla, denegarla, pedir permiso* esta útima puede ser demasiado cargante si por ejemplo se recibe un ataque. Por nuestro bien lo bloquearemos, esto quiere decir que el que manda la respuesta, no recibirá ninguna respuesta.

Cabe destacar la opción de **Reflejado**, sirve para cuando queremos aplicar la regla a la inversa, ademas se utiliza la regla inversa, cambiando origen y destino, esto por ejemplo es util por si algun virus o alquien con un troyano intenta montar unidades remotas.

Propiedades de Filtro
Direccionamiento Protocolo Descripción
Dirección de origen:
Cualquier dirección IP
Mi dirección IP
Hetlejado. Hacer coincidir paquetes con las direcciones de origen y destino opuestas exactas.
Aceptar Cancelar Aplicar

Figura 17: Reflejado sirve para crear directivas opuestas.

Por ejemplo si bloquease a partir de su dirección IP el puerto 80, y estubiese reflejado, usted no podría navegar, en cambio si no lo pone reflejado podrá navegar sin problemas, haga la prueba.

Lista de filtros IP				? ×
Un filtro IP se o	compone de múltiples filtr cciones IP y protocolos e	os. De esta forma se pu n un filtro IP.	ieden combinar múltiple	18
<u>N</u> ombre:				
No Dejar				
Descripción:			A	gregar
			M	odi <u>f</u> icar
			Y	<u>Q</u> uitar
Filtro <u>s</u> :			🔽 Usar Asistente para	a agregar
Protocolo	Puerto de origen	Puerto de destino	Nombre DNS de o	. Direcciói
TCP	Cualquiera	137	<cualquier direcci<="" td=""><td><cualqui< td=""></cualqui<></td></cualquier>	<cualqui< td=""></cualqui<>
₹				Þ
			<u>C</u> errar C	Cancelar ///

Figura 18: Ventana de nuestro filtro No Dejar y los puertos afectados.

Utilizaremos otro asistente para aplicar las reglas, sin los asistente la labor sería mas tediosa. O por lo menos mas difícil de entender.

tente para reglas de se	guridad	?
Lista de filtros IP Seleccione la lista de fill seguridad.	ros IP para el tipo de tráfico IP al que se	e aplica la regla de
Sinohayun filtro IP en en Agregar para crearu	la siguiente lista que coincida con sus n no nuevo.	ecesidades, haga clic
Listas de filtros IP:		
Nombre	Descripción	Agr <u>eg</u> ar
O No Dejar		Modificar
		Quiter
		Quitar
1		
	Z Aluán C	Canadar
	< Anaz 2	

Figura 19: Asistente para reglas a aplicar.

Si no hay acciones de filtrado en la	a siguiente lista que coincidan con sus	s necesidades,
haga clic en Agregar para crear un agregar.	ia nueva. Para ello, seleccione Usar e	el Asistente para
Acci <u>o</u> nes de filtrado:		
	⊡ sarA	sistente para agr
Nombre	Descripción	Agr <u>e</u> gar
O Permitir	Permite el paso de paquetes I	1.1 177
O Requiere seguridad	Acepta comunicación no seg	Modificar
O Seguridad de petición (opci	Acepta la comunicación segu	Quitar
• • • • • • • • • • • • • • • • • • •	-	

Figura 20: La acción de Filtrado decide que hacer con la directiva de seguridad creada.

Utilizaremos el asistente para crear una nueva acción de filtrado y le damos a Aceptar. Ya que la que nos interesa no esta creada.

Asisten	te para acciones de filtrado	? ×
Nom	i bre de la acción de filtrado Póngale un nombre a esta acción de filtrado y escriba opcionalmente una breve descripción	167
1	Nombre:	
J	Filtrado Bloquear	
[Descripción:	
Ĩ		~
		-
	< Atrás Siguiente >	Cancelar

Figura 21: Asignamos un nombre a la acción de filtrado..

Que va a ser la que nos permita bloquear.

Acción de filtrado			? ×
Opciones generales de acciones de filtra Establecer el comportamiento de la acción d	a do de filtrado.		161
C Permitir			
Bloquear			
O Negociar la seguridad:			
	< Atrás	Siguiente >	Cancelar

Figura 22: Seleccionamos Bloquear.

Asi lo que hará esta acción es bloquear las conexiones, impedir que se realicen.

Asistente para acciones de fi	ltrado	? ×
	Finalización del Asistente para acciones de filtrado de seguridad IP	
1061	Ha completado satisfactoriamente el Asistente para directivas de seguridad IP.	
	Para modificar ahora su acción de filtrado, seleccione la casilla de verificación Modificar propiedades, y luego haga clic en Finalizar.	
	Modificar las propiedades	
	Para cerrar este asistente, haga clic en Finalizar.	
	< Atrás Finalizar Can	celar

Figura 23: Ya tenemos nuestra acción de filtrado creada.

Propiedades	s de Acción de fill	rado nueva		<u>? ×</u>
Métodos de	seguridad Gener	al		
○ Permit○ Bloque○ Negoo	ir ear ciar la seguridad:			
Orden de Tipo	preferencia de méto Integridad AH	dos de seguridad: Confidencialidad	Int	Agregar
				Modificar
				Quitar
				Subir
1			F	Bajar
Confid	ar comunicación no ir la comunicación r lencialidad directa p	segura, pero respon o segura con equipo erfecta de clave de :	der siempi is no com sesión	re usando IPSec patibles con IPSec
		Aceptar	Cancela	r Aplicar

Figura 24: Dejamos tal como esta.

Como puede verse, si hubiesemos seleccionado otra como, pedir seguridad podemos habilitar mas opciones, sólo si utilizamos ciertas directivas de seguridad que se requieran.

haga clic en Agregar	para crear una nueva	a. Para ello, seleccio	one Usar el Asistente para
agregar.			
Acci <u>o</u> nes de filtrado:		L.	Ilsar Asistente nara agr
Nombre	Descr	ipción	Agr <u>eg</u> ar
○ Filtrado Bloquear			
O Permitir	Permit	te el paso de paquet	es I <u>M</u> odificar
O Requiere segurio	lad Acept	a comunicación no :	seg Quitar
O Seguridad de pe	tición (opci Acept	a la comunicación s	egu

Figura 25: Seleccionamos la acción de Filtrado que para aplicar la regla No Dejar.

Asistente para reglas de seg	uridad	? ×
	Finalización del Asistente para regla nueva Ha completado satisfactoriamente la especificación de las propiedades de su nueva regla. Para modificar ahora su regla de seguridad, seleccione la casilla de verificación Modificar propiedades, y luego haga clic en Finalizar.	
	Modificar las propiedades	
	Para cerrar este asistente, haga clic en Finalizar.	
	< <u>A</u> trás Finalizar Cance	elar

Figura 26: Y volvemos a lo mismo de antes.

Podemos crear reglas para separar los puertos, por ejemplo del tipo de protocolo TCP o UDP, en vez de tenerlas todas juntas.

opiedades de Corta	fuegos		?)
Reglas General			
Reglas de	seguridad para establecer c	omunicación con ec	juipos
Reglas de seguridad l	IP:		
Lista de filtros IP	Acción de filtrado	Métodos de a	Configuración .
🗹 No Dejar	Filtrado Bloquear	Kerberos	Ninguno
•	1	1	Þ
Agregar M	odificar Quitar	📕 🔽 Usar Asister	nte para agregar

Figura 27: Si tenemos seleccionada nuestra regla, el cortafuegos esta listo

Le damos a Cerrar, el siguiente paso será activar la Directiva de Seguridad creada.

Como mencione anteriormente es conveniente crear varias reglas de filtrado basándose en los tipos de protocolo de aplicación (los puertos)

Sino activamos la regla creada de Cortafuegos, es como si no hubiésemos hecho nada, para ello seleccionarla y darle o bien al icono del interruptor o bien con el botón derecho en asignar.

💀 Configuración de seguridad local						
<u>A</u> cción <u>V</u> er ← → 🗈 🖬 🗙 🛱 🗔 😰 🎦 🍰 🧕 🧕						
Árbol	Nombre 🛆	Descripción	Directiva asignada			
Arbol Image: Configuración de segurida Image: Configuración de segurid	Nombre Cliente (sólo responder) Cortafuegos Servidor (Pedir seguri Servidor seguro (requ	Descripción Comunicarse normalmente (Par Par Todas las tareas Eliminar Cambiar nombre Propiedades Ayuda	Directiva asignada No No No No			
I						
Asignar esta directiva; intentar hacerla activa						

Figura 28: Asignado la directiva de seguridad, activaremos todas las reglas antes creadas

Aquí teneis unos cuantos puertos y protocolos que recomiendo que chapeis, para impedir que os causen daño o os accedan sin permiso.

Nombre	Тіро	Puerto	Protocolo
Netbios (RPC)	Windows	135	TCP / UDP
Netbios Nombre	Windows	137	TCP / UDP
Netbios Datagrama	Windows	138	TCP / UDP
Netbios Sesion	Windows	139	TCP / UDP
Microsoft-ds+	Windows	445	TCP / UDP
NetBus	Troyano	12345	ТСР
BackOriffice	Troyano	31337	UDP

No obstante vosotros podréis ver que puertos tenéis activos, es decir os pueden acceder desde el exterior. Para esto existe un comando que dice que puertos están activos... basta con ejecutar:

$Inicio \rightarrow Ejecutar \rightarrow cmd$

Una vez dentro del intérprete simplemente:

netstat -an

Existe un listado extenso de puertos, definidos por la IANA, esto es una descripción de TODOS, pongo la referencia a título ilustrativo para que veáis la cantidad de puertos que existen.

Listado Completo de Puertos

Revisado a 11 de Julio de 2003. Si encuentra algún fallo o algo no queda lo suficientemente claro, por favor escriba a i72maprj@uco.es