

## BIENVENIDO A ESTA GUIA SOBRE **KERIO** DE UN HUMILDE SERVIDOR:

En primer lugar dar las gracias por estar leyendo estas palabras, señal de que no he trabajado en vano. Procurare explicar los pasos desde que alguien decide ponerse un cortafuegos en el pc, hasta que lo deja ya instalado y configurado.

Asi mismo autorizo este manual sin licencia alguna ni hostias a la libre distribucion. Tan solo pediria que se respete el hecho de mi autoria como creador del mismo. La informacion debe ser libre y al alcance de todos. Muerte al monopolio de Micro\$oft.

Saludos desde aqui a mis amigos de los foros de ya.com gracias a los cuales he aprendido mucho en estos dos años que llevo metido en la informatica como forofo de la misma. Parte de los conocimientos adquiridos se deben a ellos que en sus horas de inestimable y desinteresada ayuda hacen posible que gente que entra a este apasionante mundo pueda poco a poco salir a delante con mas exito que desesperacion y fracasos.

Saludos en especial para:

**Toni** mi gran amigo con el que se que siempre podre contar.

**Berta** quien me soporto en mis comienzos con el pc y no fui justo con ella.

**Dvdrw** mi compi de foro :-)

**Suicida** e **Icarus** del foro hackers, grandes donde los haya.

**Edgtho** de los foros de programacion y delphi.

**Antonio Caravantess** del foro Consultas Informaticas.

**Splitter77**, **Adolpheus** y **Esteban 1950** del foro linux.

Muy en especial para mi amiga **Samantha** de la cual hace ya tiempo que no se nada y que tanto me apoyo en mis inicios con linux.

A todos ellos, a todos los que se me pase citar de los foros y a todos los lectores, gracias por vuestra ayuda, amistad y tiempo.



**SALUDOS DE ZORTH.**

--FDZ GROUP--

**VISITA MI FORO EN:**

<http://foros.inicio.tiendapc.com/jsp/JVforums.jsp?D=readforum&F=45421>

[mailto: zorth@spanish.as](mailto:zorth@spanish.as)

---

-----

## **PUNTO 1.**

### **QUE ES UN CORTAFUEGOS?**

Un cortafuegos es un programa de software para nuestro caso particular (un cortafuegos puede llegar a ser incluso todo un ordenador que esta al frente de una red de ordenadores, pero nosotros usaremos el cortafuegos de soft), el cual se instala en el sistema operativo e impide que el trafico no permitido por nosotros desde internet a nuestro sistema y viceversa sea controlado e incluso frenado.

El cortafuegos es imprescindible para alguien que tiene adsl en monopuesto o bien conexion cable, que se pasa el Sto. dia conectado a internet. Incluso es muy recomendable para quienes tan solo chateen una hora por la tarde antes de cenar. No solo nos hara estar mas tranquilos con nuestra seguridad, sino que ocupa pocos recursos del sistema y nos salvaguarda de tener sin saberlo troyanos, spywares, aplicaciones saliendo o entrando sin control, posibles ataques **dos** (denegacion de servicio traducido) por parte de algun capullo online.... etc.

Podria ahora alargar este primer punto con explicaciones largas y complicadas sobre que es un puerto, un protocolo, comunicaciones y accesos en una red... pero eso lo dejare a voluntad del lector para que use google ( <http://www.google.com> ) y se informe con todo detalle. En este manual dare por sentado que se ha leido un poquito sobre esto antes o bien, se leera para comprender y asimilar mejor lo que aqui se va a tratar.

## **PUNTO 2.**

### **QUE CORTAFUEGOS USO?**

Aqui queria llegar yo. No recomiendo el uso de zone alarm, black ice, norton y demas cortafuegos ya que dejan MUCHO que desear. Simplemente, como veremos mas adelante comparados con kerio, son programas que apenas pueden ser configurados y adaptados a las necesidades concretas de cada uno.

Por eso, en esta guia vamos a tratar con el mejor cortafuegos que hay para windows --> **kerio firewall** antes conocido por **tiny firewall** hasta que desaparecio con la version 2.1.15 ya que sus programadores abandonaron la tiny software para establecerse por su cuenta en kerio software. Kerio, lleva el corazon y alma que hicieron de tiny firewall el mas robusto cortafuegos para windows pero con adaptaciones al nuevo protocolo ipv6.

## **PUNTO 3.**

### **DE DONDE CONSIGO KERIO?**

Bien, iremos a la pagina de <http://www.kerio.com> y veremos en downloads la posibilidad de bajar kerio firewall. Cuando lo hayamos bajado, veremos que el programa es freeware solo para el uso personal. Para empresas, colegios, entidades gubernamentales, etc, es obligatorio pasados 30 dias que de seguir usandolo se registre y pague licencia. No sera ese nuestro caso.

Una vez instalado el programa nos pedira de reiniciar el pc y asi lo haremos. Recien rebotado el sistema el primer signo de por fin tener un cortafuegos sera ver el log de kerio apareciendo unos segundos. Ahora, fijate que en el systray o barra de tareas de windows, junto al reloj vamos, tienes un nuevo icono con forma de escudo azul. Ahora, no abras ninguna ventana del navegador ni abras correos ni nada por el estilo, ha llegado la hora de aplicar lo que en este guia tratare de explicar paso a paso. Asi que presta atencion porque kerio sera junto a tu antivirus el programa que puede salvar tu disco duro, tu pc o simplemente tu estado online de ataques, intentos de infiltracion a tu sistema, troyanos y demas paranoias en la red.

## PUNTO 4. FAMILIARIZANDOSE CON KERIO.

### **LA VENTANA DE MONITORIZACION.**

Ahora lo primero que haremos para empezar a tomar confianza con kerio sera precisamente picar dos veces ese nuevo icono de escudito azul. Veremos ahora, que se nos abre una ventana de monitorizacion de los servicios y las conexiones establecidas por nuestro sistema. Es como una interfaz grafica mucho mas completa del comando netstat de msdos.

Application	Protocol	Local Address	Remote Address	State	Creation Time	Rx (Bytes)	Rx
CUTFTP32.EXE	TCP	0.0.0.0:2980	204.26.89.194:5525	Connected Out	02/Sep/2002 21:38:19	3227	
CUTFTP32.EXE	TCP	[REDACTED]:2984	204.26.89.194:5524	Connected In	02/Sep/2002 21:38:32	51115404	
IEXPLORE.EXE	UDP	127.0.0.1:3259	0.0.0.0	Listening	02/Sep/2002 22:10:49	177	
LSASS.EXE	UDP	[REDACTED]:500	0.0.0.0	Listening	01/Sep/2002 06:35:07	0	
MPROXY.EXE	TCP	0.0.0.0:8088	0.0.0.0	Listening	02/Sep/2002 13:40:04	0	
MSMSG.S.EXE	UDP	0.0.0.0:3168	0.0.0.0	Listening	02/Sep/2002 21:58:05	0	
MSMSG.S.EXE	UDP	[REDACTED]:3169	0.0.0.0	Listening	02/Sep/2002 21:58:05	0	
MSMSG.S.EXE	UDP	[REDACTED]:7363	0.0.0.0	Listening	02/Sep/2002 21:58:06	0	
MSMSG.S.EXE	TCP	[REDACTED]:12050	0.0.0.0	Listening	02/Sep/2002 21:58:06	0	
MSMSG.S.EXE	UDP	127.0.0.1:3172	0.0.0.0	Listening	02/Sep/2002 21:58:29	0	
MSMSG.S.EXE	TCP	0.0.0.0:3171	64.4.12.131:1863	Connected Out	02/Sep/2002 21:58:16	24644	
MSTASK.EXE	TCP	0.0.0.0:1026	0.0.0.0	Listening	01/Sep/2002 06:34:58	0	
PERSFW.EXE	TCP	0.0.0.0:44334	0.0.0.0	Listening	01/Sep/2002 06:34:59	0	
PERSFW.EXE	UDP	0.0.0.0:44334	0.0.0.0	Listening	01/Sep/2002 06:34:59	0	
PERSFW.EXE	TCP	0.0.0.0:44334	127.0.0.1:3343	Connected In	02/Sep/2002 22:34:38	3404	
PFWADMIN.EXE	TCP	0.0.0.0:3343	127.0.0.1:44334	Connected Out	02/Sep/2002 22:34:38	107706	
SERVICES.EXE	UDP	0.0.0.0:1027	0.0.0.0	Listening	01/Sep/2002 06:35:00	0	
SVCHOST.EXE	TCP	0.0.0.0:135	0.0.0.0	Listening	01/Sep/2002 06:34:55	0	

TCP Listening: 6    TCP Connected: 5    UDP Listening: 10    Total Rx speed: 15.11    Total Tx speed: 1.52

En la foto donde he tachado en rojo mi propia ip :-), podemos ver las conexiones que YO tenia establecidas en el momento en que capture la foto. Por pasos vemos que:

**Application:** es la aplicacion o proceso que tiene una comunicacion establecida.

**Protocol:** es el protocolo que usa dicha aplicacion, los usuales son tcp o udp.

**Local Address:** es la ip local logicamente, con su puerto si asi se desea tener como es mi caso.

**Remote Address:** la ip remota donde se tiene una conexion establecida. Si es como se ve en la foto una ip formada con 0.0.0.0 logicamente es que aun estando el servicio a la escucha (listening) aun no tiene una conexion establecida.

**State:** es el estado del servicio o aplicacion:

- listening: comunicacion no establecida con nadie pero el servicio/puerto esta pendiente o escuchando.

- connected out: el servicio esta establecido a un host remoto y el trafico es de salida (out=hacia fuera)

- connected in: el servicio esta establecido de un host a nosotros y el trafico es de entrada (in=entrada)

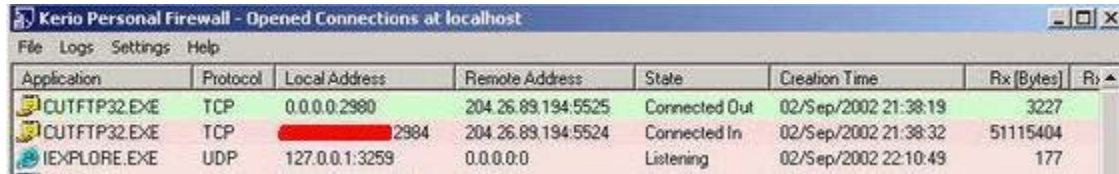
**Rx/RxSpeed:** recibidos bytes (Rx bytes=cantidad) a la velocidad x (RxSpeed kbytes/segundo)

**Tx/RxSpeed:** transmitidos bytes (Tx bytes=cantidad) a la velocidad x (TxSpeed kbytes/segundo)

De todo esto, lo mas importante verdaderamente es observar de vez en cuando que SERVICIOS tenemos activos, usando que PROTOCOLO y por que PUERTO LOCAL y si esta activada una conexion remota de entrada (in o incoming) o de salida (out u outgoing) y hacia que IP REMOTA.

Asi, si podremos ver en todo momento si algun "lamer" o algun "hacker" XDDD, esta conectando a nuestro sistema por que puerto remoto a que puerto local y que servicio tenemos abierto que lo permite.

Concretamente, si observamos la foto de antes justamente aqui--->



Application	Protocol	Local Address	Remote Address	State	Creation Time	Rx (Bytes)	Rx
CUTEFTP32.EXE	TCP	0.0.0.0:2980	204.26.89.194:5525	Connected Out	02/Sep/2002 21:38:19	3227	
CUTEFTP32.EXE	TCP	127.0.0.1:2984	204.26.89.194:5524	Connected In	02/Sep/2002 21:38:32	51115404	
IEXPLORE.EXE	UDP	127.0.0.1:3259	0.0.0.0	Listening	02/Sep/2002 22:10:49	177	

.... podremos ver que tenia el servicio de CUTEFTP32.EXE usando el protocolo tcp desde mi puerto local 2980 conectado a una ip remota 204.26.89.194 por el puerto remoto 5525. Sin embargo, IEXPLORER.EXE que usaba en ese momento el protocolo udp por mi localhost (127.0.0.1) y desde mi puerto local 3259, NO tenia una conexion activa. Se puede ver es estado de "listening" o escuchando.

Ahora, picaremos al lado de **File** la pestaña **Logs** y veremos que se abre dos mas: **Statistics** (estadisticas) y **Firewall Log** (log del cortafuegos). Piquemos a log y veremos eso mismo, el archivo donde **kerio** guardara y registrara todas las actividades que haya realizado. Esto puede ser muy util para saber que ha pasado mientras nosotros estabamos por ejemplo, jugando en red, o viendo la TV mientras el pc trabajaba haciendo cualquier cosa como tambien para tener constancia de cualquier evento. Todo queda ahi registrado. Hay que señalar, que el servicio de log de kerio funcionara si asi lo deseamos indicandolo al programa en cada regla que tengamos como veremos mas a delante en este manual.

El archivo log puede ser localizado en la carpeta de instalacion de kerio por defecto:

C:\Archivos de programa\Kerio\Personal Firewall\filter.log

Ahora, en la pestaña **Settings** podemos configurar la vista de la monitorizacion como mas nos plazca... viendo solo el nombre del host o su ip, solo el host/ip sin el puerto o con el puerto... etc. Tal como lo tenia configurado en el momento de la foto de arriba, era SOLO con las opciones picadas de **Dont resolve domain names** y **Dont resolve port names**.

### CONFIGURANDO LAS PRIMERAS OPCIONES.

Ahora vamos a darle caña al kerio XDD. Para empezar, en el icono de la barra de sistema lo vamos a picar con el boton derecho. veremos que se nos aparece una ventanita con varias opciones:

**Exit:** salir del programa

**About:** info sobre la version del kerio y poco mas.

**Help:** la ayuda de kerio jeje. Se supone que si lees esto es que no se te da bien el ingles :-)

**Administration:** lo dice ya todo la propia palabra y es donde iremos ahora en este punto.

**Firewall Status:** la ventana de monitorizacion de las conexiones que hemos visto ya.

**Stop all traffic:** parar todas las conexiones. Osea, como si desenchufaramos el cable del modem, lo mismo. Es una opcion de "emergencia" si nos asustamos ante unas cosas muy raras como que el raton se mueva solo o escuchemos estupefactos voces ultratumba emitiendo gemidos por los speakers, XDDD.

Pues bien, nosotros iremos ahora a la opcion **Administration** donde se nos abra una nueva ventana.

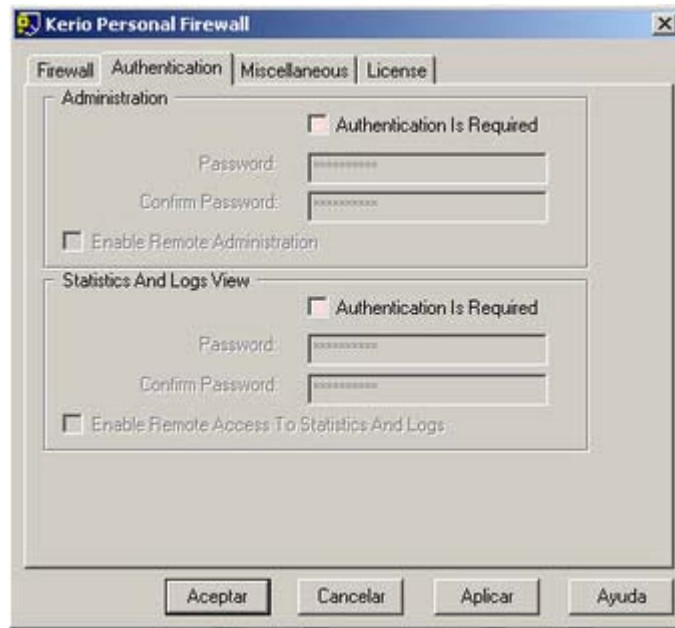


Ahora, lo que vemos tras picar a administration es como debe estar kerio en esta primera ventana para que este operativo. Siempre la pestaña de Firewall Enabled (cortafuegos activo).

Mirando en la barra que se desplaza a 3 posibles posiciones vemos que la del medio es la de por defecto, **Ask Me First** (preguntame primero). Se puede bajar al nivel de **Permit Unknown** (permitir a desconocidos) lo cual no es nada aconsejable, pues si aplicas y aceptaras este cambio significaria que tu cortafuegos no hara nada por impedir cualquier tipo de trafico de entrada o salida. Y por ultimo, si subieramos la barra hacia la primera posicion donde rezara **Deny Unknown**, esto significara que SOLO y EXCLUSIVAMENTE podra tener conexion cualquier servicio cuya/s regla/s esten totalmente definidas. Kerio, no hara ninguna pregunta pues se basara en las reglas establecidas y cualquier intento de conexion de cualquier tipo sera denegado SIN preguntar.

Esto, al menos que se tenga "perfectamente" configurado kerio no es aconsejable tenerla como opcion por defecto ya que se nos podria dar el caso de querer establecer una conexion o un programa que necesite actualizarse... cualquier cosa y de no percatarnos de que aun no hemos hecho reglas para este evento, kerio no nos avisara y estara por defecto, negandolo todo.

Ahora, picaremos a la 2ª pestaña, **Authetication**.

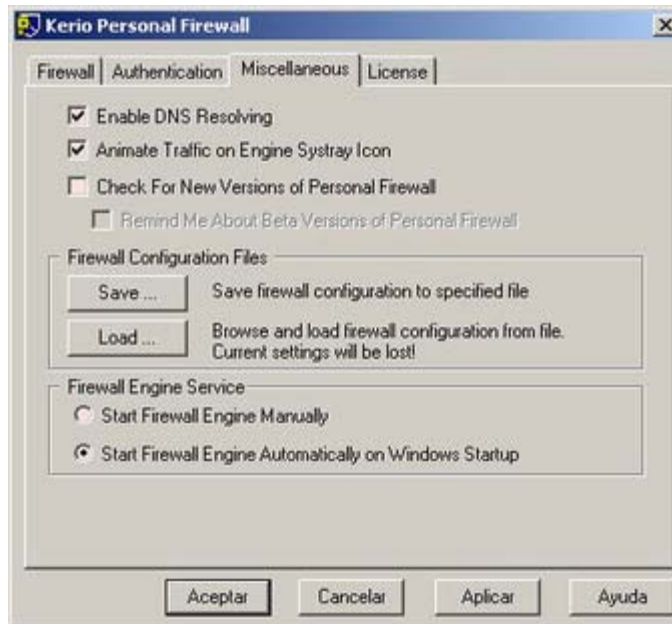


Estas opciones solo nos va a interesar si queremos poner contraseña a nuestro kerio y que nadie pueda cambiar la configuracion de como la tegamos nosotros. Tan solo le puede interesar a la persona que comparta su pc con mas usuarios.

De todas formas, vemos que las opciones a picar son tan solo para proteger la configuracion de las reglas en la primera seccion y que nadie pueda borrar los logs y estadisticas generados por kerio si activamos la contraseña de la segunda seccion.

La opcion de "Enable remote aministration/access log..." tan solo es interesante si uno se va a conectar remotamente a su propio pc por ejemplo, desde el curro y desea en ese momento pasarse pongamos unos archivos pero tal y como estan las reglas y lo cañero que es kerio para esto, pues no nos va a dejar. Entonces, podriamos acceder a la re-configuracion romota si hemos activado esta casilla. Esto, por cierto, no es nada aconsejable para un usuario casero (home user) siendo el unico que toca el pc y menos, si no va a acceder remotamente por cualquier tipo de programa o metodo a su propio pc.

Pasemos ahora, a la 3ª pestaña, **Miscellaneous**.



Tal como aparece en la foto es como mejor se puede dejar kerio en este punto. Las posibles opciones son:

**Enable DNS Resolving:** kerio resolvera por ejemplo en el log que genera como en la monitorizacion, la dns de una ip que intente conectar con nosotros o bien, que nuestro sistema desee conectar con ella. Va muy bien tenerla activada. Pongamos un ejemplo: ip 12.12.12.12 intenta conectar al sistema... pero con esta casilla seria... ip 12.12.12 dns.terra.es bla bla bla....

**Animate traffic on Engine Systemtray Icon:** lo dice todo ya. Si esta picada hara que aparezca la flechita en verde o rojo en el icono de kerio. Asi pues, si la flecha esta en verde es que tenemos un trafico originado y kerio lo permite. Si la flecha esta en rojo, kerio tiene trafico activo pero lo esta negando. Es util pongamos, en un caso por ej., que alguien intente "atacarnos" o escanear todos nuestros puertos desde el primero al ultimo pues veriamos que la flecha de kerio parpadeara en rojo y sin parar... ojo!! algo sucede y kerio esta negando ese trafico. Lo suyo, sera ver en el archivo log que narices sucede y que ip, que puertos... etc.

**Check for new versions.....bla bla:** kerio en cada inicio del sistema buscara en su web si hay alguna actualizacion disponible. No recomiendo esta opcion, ya que mejor nos ocupamos nosotros de ver si hay o no nueva version.

En la segunda seccion vemos que dice: **Firewall Configuration Files.** Aqui muy poco que comentar aunque es muy importante. Con load (cargar) o save (guardar) podemos mismamente, cargar una configuracion de kerio, reglas incluidas, que alguien nos deje (no recomendado para nada) o las que en su dia grabamos para tenerlas como copia de seguridad por ej.. Al picar cualquiera de ellas, veremos que nos pide un nombre de archivo.conf para cargar o bien, si vamos a salvar nuestra configuracion de kerio, nos pedira el sitio donde guardar y el nombrearchivo.conf.

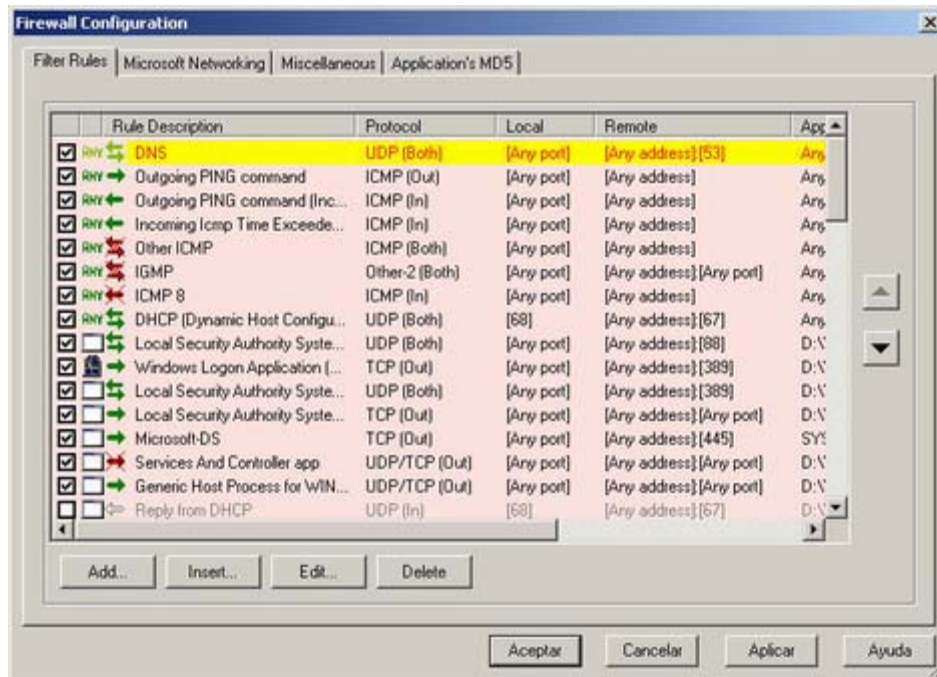
Y por ultimo, en **Firewall Engine Service**, tan solo elegimos si kerio arranca en cada inicio del sistema (recomendado solo para los de adsl/cables conexion 24 h) o manual, es decir, ejecutando kerio nosotros mismos antes de enchufarnos al vicio de internet como locos :-p

La ultima ventana de este apartado seria **License** y como unico contenido "registration". Si somos un home user, osea, un tio/a de estar en casita con el guindos, no tenemos que registrar kerio y pagar licencia. Esto solo sera necesario para empresas, colegios, unis y demas entidades gubernamentales.

## **PUNTO 5.** **CONFIGURANDO KERIO MAS EN PROFUNDIDAD.**

Ahora, volvemos a la primera pestaña donde pone firewall y picamos **advanced...** para entrar en el super distraído mundo de las famosas "reglas" XDDD.

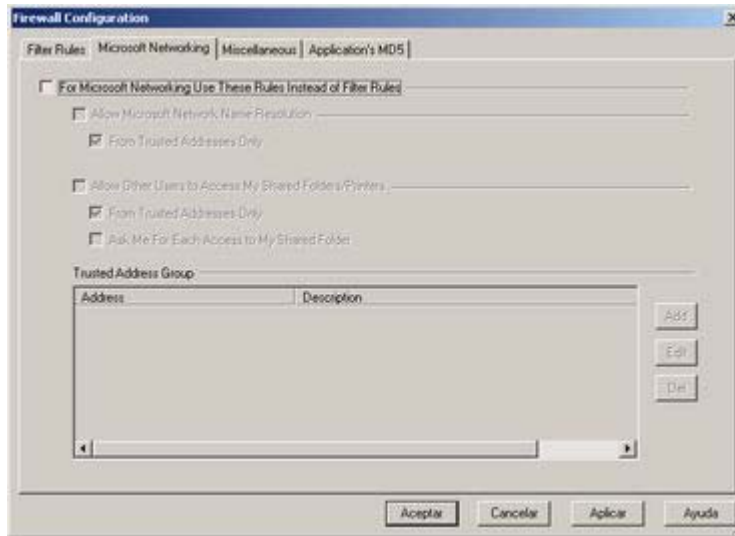
Nos encontraremos con algo parecido a esto



asi que antes de adentrarnos en profundidad, comentare de esta primera vista que cada linea de las que arriba se ven, es una regla o llamadle filtro. los posibles aceptar/cancelar/aplicar/ayuda creo que no hara falta que los explique :-)

- **Add...**: sirve para añadir una nueva regla que hagamos.
- **Insert...**: exactamente para lo mismo. usaremos siempre Add...
- **Edit...**: sirve para editar como ya dice la palabra. Se usara para modificar el contenido de una regla ya creada.
- **Delete**: el deporte favorito del usuario inexperto, jejeje, borrar lo que no conoce. Pues eso, borrar una regla.

Ahora, picamos a la 2ª pestaña que dice **Microhof Networking** y nos saldra otra ventanita muy chula



en la que se pueden configurar varios parametros para el tema de tener nuestro sistema en red con otros pcs. Yo como podeis ver lo tengo todo off, sin nada seleccionado ya que no tengo porque compartir ningun recurso ni conexion con nadie. No sera este mi caso, el de otro usuario que SI tenga su pc en red con otros.

Si no tienes tu pc en red saltate esta parte y sigue la guia mas adelante, si tu pc esta en red te interesara leer un poco sobre esto.

Si tu pc forma parte de una red y deseas que kerio no impida que este muestre su nombre de host, grupo trabajo de ntbios etc... deberas picar la primera pestaña, la de **For Microsoft Networking Use These....** y picar la pestaña de **Allow Microsoft Network Name Resolution**. Aqui es muy importante picar las subpestañas que dicen **From trusted Adresses Only** ya que luego, como veremos solo confiara esta informacion o permitira la entrada/salida de recursos compartidos para las ips/rangos que definamos como de "confianza".

Ahora, donde pone **Allow Others Users to Access my Shared folders/printers** si picamos esta opcion, le diremos a kerio que si alguien intenta acceder a nuestros recursos compartidos de tenerlos, sean una carpeta con 3 fotos o sea toda la unidad C:\, no ponga objecion y lo permita. Como ya he comentado, ante este caso es imprescindible picar aqui de nuevo **From trusted Adresses Only** y a continuacion picando Add... añadiremos las reglas que correspondan.

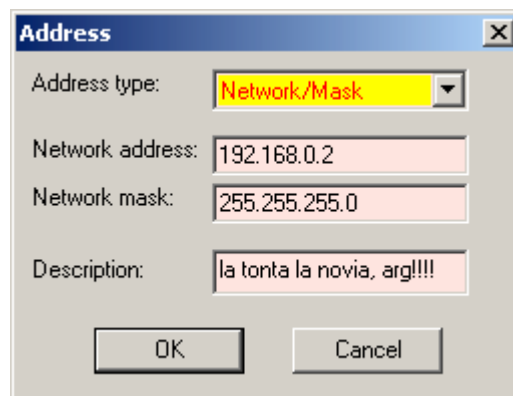
En la ultima pestaña de la comparticion de archivos donde pone **Ask Me For Each...** le indicaremos a kerio que en el momento que detecte una conexion a nuestros archivos compartidos, nos pregunte si lo permitimos o no en ese momento. Por ejemplo, si tienes el pc de tu novia con el tuyo en red y ahora, no te va bien que tu novia se meta a subir/bajar archivos a tu disco porque estas con una coleguita muy...umm con netmeeting activo y necesitas "intimidad", banda ancha... lo que sea XDDDD.... pues le diriamos a kerio que deniegue en ese momento el intento de compartir nada que andamos "ocupados" cuando nos saliera la tipica ventanita de Aviso del cortafuegos. XDD. Es solo un ejemplo.

Bueno, entonces si hemos seleccionado la primera seccion como si hemos seleccionado la segunda para que no solo se identifique como parte de una red X, si no que encima compartiremos recursos y/o impresora, y de nuevo, hemos picado la/s opcion/es de **From trusted Adresses Only** ha llegado ahora el momento de decir que demonios son las "trusted adress" o "direcciones acreditadas", vamos, las ips de confi.

Para darle a kerio las ips de confianza ya que solo queremos que estas y las de la red a la que pertenezcamos sepan de nuestra andadura por la misma y/o puedan acceder a nuestro path compartido (recursos), veremos que a la derecha hay 3 posibles opciones: add (añadir) edit(editar/modificar) y del (borrar).

Aqui, tan solo pondre un par de ejemplos que supongo deben bastar para el caso, ya que sospecho que el 90% de los usuarios de kerio NO compartiran demasiadas cosas en una red. (ojo!! esto no significa ni tiene nada que ver para nada con compartir a traves de programas como los kazaa o edonkeys de turno, sino exclusivamente para los recursos compartidos de windows/microsoft).

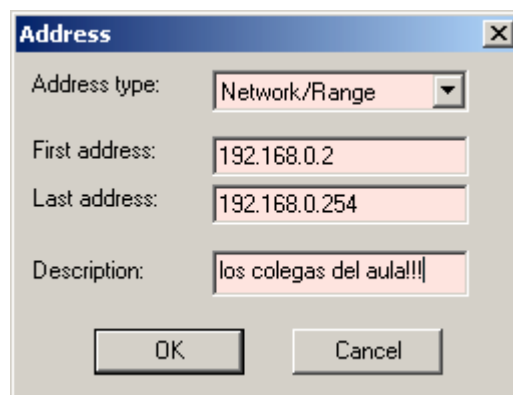
pongamos que nuestra novia que tiene ip interna 192.168.0.2 y logicamente, usando la misma mascara de subred, va a conectarse a nuestro sistema y queremos que kerio lo permita asi.... picamos add.. y esto es lo que pondremos



The screenshot shows a dialog box titled "Address". It has a dropdown menu for "Address type" set to "Network/Mask". Below it are two text input fields: "Network address" containing "192.168.0.2" and "Network mask" containing "255.255.255.0". A "Description" field contains the text "la tonta la novia, arg!!!!". At the bottom, there are "OK" and "Cancel" buttons.

asi, permitimos que una ip/mascara subred concretas dandole a ok, puedan acceder a formar parte de las "adress trusted" o direcciones de confianza.

Otro ejemplo seria que pongamos, que formamos parte de un aula de informatica por decir algo... y nos vamos a compartir mazo cosas unos con otros, osea, que formamos realmente parte de una red bien guapa con monton de pcs pasandose unos a otros historias. Para este caso, no definiremos uno por uno ip a ip, sino que seleccionariamos esta otra opcion



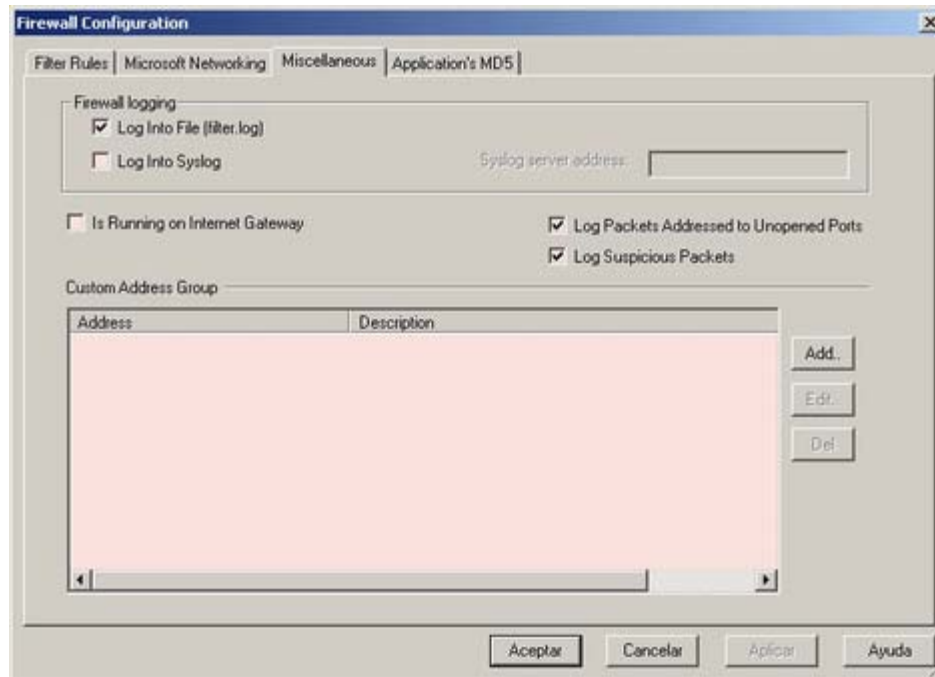
The screenshot shows a dialog box titled "Address". It has a dropdown menu for "Address type" set to "Network/Range". Below it are two text input fields: "First address" containing "192.168.0.2" and "Last address" containing "192.168.0.254". A "Description" field contains the text "los colegas del aula!!!". At the bottom, there are "OK" and "Cancel" buttons.

Ahora vemos que hay un cambio tan solo en que ponemos la primera ip de la red y la ultima y en esas 254 ips, esta cada uno de los pcs de los colegas que bla bla bla. Aceptamos pulsando ok y la regla estara creada.

Con esto, podemos agregar las ips de confianza por las cuales basara kerio sus criterios de

deteccion de conexiones. Si alguna ip acreditada intenta entrar a nuestro equipo y asi pues consta para kerio, este no impedira que esto suceda. Hay que tenerlo muy en cuenta a la hora de trabajar en red con recursos. Y como ni yo trabajo con recursos compartidos como ya he dicho, ni creo que la mayoría de vosotros que leéis esto lo hagáis, doy por finalizado el tema de los recursos de guindos y kerio por medio :-p

Ahora seguimos con la siguiente pestaña **Miscellaneous**



Esto debe ponerse tal y como lo tengo yo aqui para llevar un control en el log de kerio casi total de intentos de conexion o paquetes recibidos a puertos cerrados. No explicare sobre esto demasiado ya que no tiene mayor complicacion que seleccionar las casillas que se ven en la foto picadas para que kerio registre en su propio log las actividades a puertos cerrados (unopened ports) y los paquetes sospechosos (suspicious packets). Arriba, si en lugar de seleccionar como esta en la foto en **Log into file (filter.log)** seleccionaramos tambien **Log Into Syslog** le indicariamos a kerio que queremos tambien que registre su actividad de bloqueo con destino a nuestro sistema tambien en el log del guindos propio. Pero es una opcion a no tener en cuenta.

Por ultimo, aqui solo destacar la opcion de **Is Running on Internet Gateway** la cual indica a kerio que nuestro sistema esta haciendo las veces de gateway. Esto, no hay que picarlo JAMAS a no ser que... pongamos un ejemplo:

Pongamos que tienes una conexion a internet con una sola ip publica pero que al mismo tiempo, estas conectado con mas ordenadores en red. Asi pues, podrias tener tras de ti y con ips de rango interno conectados con tarjetas de red una serie de pcs PERO el unico que tiene el modem, el router o la conexion a internet eres TU. Si estas haciendo de pasarela para que los otros pcs puedan a traves tuyo entrar a internet, entonces puedes y debes activar esta opcion para indicarle a kerio que las **Trusted Adresses** de las que antes hablabamos recuerdas no??, son las ips a las que tu haras de gateway. Por eso, aqui deben ponerse de nuevo las Trusted Adresses o ips de confianza a las cuales tu haras de Servidor de acceso a internet, osea, de gateway.

Un ejemplo practico seria que tienes conexion a internet con el isp (proveedor de acceso a

internet, traducido) Fdz Group Telecommunications Inc. ( XDDDD ) y que este servidor de acceso a internet te da tu ip y tu router o modem de turno. Pero por el motivo que sea, tienes una ip 10.10.10.10 y quieres que por esa ip ya que te han dado con ancho de banda de 2Gb!!! jejeje, se conecten los pcs de tu primo antonio y la pesada de la novia :-). Pues bueno, se podria configurar kerio para que las ips de rango interno que seran las que se les asignen a los otros pcs en red del tipo 192.168.0.x sean las que pueden usar internet pasando por tu propia ip y de ahi a internet. Para esto, tan solo hara falta saber las ips de cada pc y en Add... meter la ip de turno y listos. Las que configuremos aqui seran las ips que puedan pasar por nosotros siendo de nuevo, nosotros mismos el gateway a internet. Esto he de indicar que puede ralentizar bastante el flujo de datos a los pcs de la red, ojo!. Pero supongo que sereis muy pocos los que os encontréis en esta situacion y todo lo que aqui se explica es solo aplicable a kerio como cortafuegos, no que kerio haga de servidor como haria un pcanywhere de symantec o un winroute de keriosoftware... jeje.

### Picando ahora la ultima pestañita **Application´s MD5**

Esta ventana ultima tan solo sirve para que kerio nos muestre las firmas MD5 de cualquier programa que haya registrado su trafico de entrada/salida en nuestro sistema. Osea, kerio cada vez que algun programa tiene actividad de entrada/salida de datos registra el ejecutable con una firma la cual como vereis es una cadena alfanumerica de letras y numeros. Si el ejecutable fuera "alterado" o sustituido por otro nuevo, kerio no permitiria la comunicacion de ese programa hasta que nosotros no le dieramos el visto bueno. Esto, es asi pongamos el caso de actualizar un programa como un editor de fotos de la version 1.0 a la 1.1. Kerio, se percatara de este cambio comprobando la firma MD5 y como no coincide la firma que tenia para la version 1.0 con la que ahora tiene de la 1.1... nos dara la alerta. En este caso con tranquilidad aceptaremos el cambio.

Lo mismo puede pasar si actualizamos pongamos, el internet explorer mierdas M\$, tambien nos avisaria que iexplorer.exe bla bla bla ha sido cambiado. Responderiamos que si. Lo interesante, raro y tal vez jodido, seria que nos empezaran a saltar alertas de cambios de firma MD5 en mazo de ejecutables sin nosotros, haber modificado ni actualizado ningun programa y de un dia para otro. Esto, sin lugar a dudas es muy mala señal, ya que seria lo que podria pasar si cogemos un virus que nos altere los .exe de nuestro sistema.

\*Desde aqui hare un llamamiento de concienciacion para que el personal que lea esta guia y aun este usando como gestor de correo Outlook express se lo siga pensando un poco... es el gestor de correo con mas problemas y fallos de seguridad que puedes usar. Al menos, recordar siempre que en sus herramientas y opciones, seleccionar la opcion de "impedir que se puedan abrir adjuntos que contengan virus" y desactivar "la vista previa al leer los msg's" ok?

### **PUNTO 6.** **FILTROS O REGLAS, EL ALMA DE KERIO.**

JEJEJE, ha llegado sin lugar a dudas mi parte favorita de la guia... las reglas, lo que si y lo que no, lo que entra y lo que sale !!?, (uys... suena morboso eso de lo que entra y sale XDD).

Para empezar voy a poner los conceptos mas basicos de las palabras con las que hemos de habituarnos y comprender para crear nuestras reglas personalizadas.

### **DICCIONARIO DE TERMINOS.** **RECURRE AQUI CUANDO TE SALTE LA DUDA CON LAS REGLAS MAS ADELANTE :-)**

- **Isp:** es el servidor de acceso a internet. Si tienes tarifa plana con terra, tu isp es terra.
- **Host:** es propiamente un pc con un sistema conectado a una red con su ip y configuracion de red.
- **LocalHost:** adivinalo... si?? Muy bien, el localhost es el pc que tienes frente a tus morros. :-D
- **Filter Rule:** tambien llamada rule, regla, filtro... da igual. La regla es un patron de

comportamiento concreto ante una situación determinada... otia, que bien me ha quedado!. jeje.

- **Protocol**: es un protocolo por el cual dos pcs "hablan" y se entienden. Verdad que yo escribo en español para que tu que lees esto me entiendas?? Pues al igual que yo hablo el "protocolo" español para que entiendas lo que escribo, tu pc hablara en "tcp", "udp", etc etc, para que otros se entiendan con el. Asi pues, se puede quedar definido como un "idioma" para la comunicacion entre pcs.

- **Guindos**: el sistema que todos criticamos y maldecimos pero que a nuestro pesar aun seguimos usando a diario XDDDDD. Lease Windows.

- **Local**: ni mas ni menos, que todo lo concerniente a nosotros, a nuestro sistema y kerio.

- **Remote**: el mas alla..... jeje. Es solo eso, el host remoto de turno este donde este. Donde estara ella que no la encuentro??? XDD

- **Port**: puerto. Un sistema usara cualquiera de los 65535 puertos.... creo que son esos concretamente aunque puerto mas o menos..... para establecer procesos de comunicacion. Cualquier programa o aplicacion que necesita de otra dentro de tu propio sistema asi como a traves de la red, ha de canalizar esa informacion por un puerto de salida local a uno de entrada remoto y viceversa para el otro host. Los puertos no son fisicos, osea, no son los usb de la torre o los ps2 del teclado y el raton, son "virtuales". Tambien comentare que desde el puerto 0 al 1024 son puertos fijos, osea, que el propio sistema a cada uno les da una utilidad concreta, mientras que a partir del 1025 en adelante, cualquier aplicacion se puede apropiarse momentaneamente de ese puerto para hacer uso de el. Se les conoce como puertos dinamicos. Lee mas sobre puertos en Google, tienes lectura para aburrir a un Santo. :-)

- **Packets**: paquetes. Los paquetes de datos son las pequeñas partes en que los protocolos dividen la informacion que va de un lado a otro por la red. Estos packets siempre llevan un destino de llegada al igual que un remitente de salida, de ahi que los paquetes vayan como un tren con sus vagones, esta el de cabecera que guia al resto desde un punto inicial a otro final. Un packet podria ser asimilado para nosotros como **h o l a** que por si sola ni la **h**, ni la **o**, ni la **l** ni la **a**, tienen sentido alguno, pero que todas juntas son una palabra. Valga el ejemplo :-)

- **Out/outgoing**: significa hacia fuera o saliendo. cuando vemos esto, entenderemos que kerio permitira o bloqueara una comunicacion "outgoing" dandonos a entender que sale de nuestro sistema hacia una ip cualquiera.

- **In/incoming**: entrando o hacia dentro. Solemos verlo tanto en las reglas a configurar como en las ventanas de alerta. Desde una ip remota cualquiera hacia nuestro sistema.

- **Both directions**: si hemos dicho que incoming es de entrada a nuestro sistema y outgoing es saliendo de el, pues **both** es en ambas direcciones, tanto de salida como de entrada.

- **Single adress/single ip**: ip unica o direccion simple. No tiene mas misterio :-)

- **Any ip/any adress... etc**: poco a comentar mas que any es lo mismo que algun o alguno/a. Entonces any ip es alguna ip, any adress es lo mismo que alguna direccion o alguna ip cualquiera, sin hacer distinciones. A kerio si le decimos **any** en algun momento para definir una regla, le diremos que "cualquiera".

- **Any port**: lo mismo, cualquier puerto, sin hacer distinciones de alguno en concreto.

- **Network/Mask**: esta es una opcion a elegir en la configuracion de reglas. Significa que especificaremos una ip mas su mascara de subred. Por ejemplo, si tu ip es 10.10.10.10 y tu mascara de subred es 255.255.255.255 pues tu network mask es esa justamente:  
10.10.10.10/255.255.255.255

- **Network Range**: si ya suponemos que network va relacionado con la ip, pues supondremos que una network range es lo mismo que un rango de ips. Por ejemplo, recuerdas al grupillo del aula de informatica del caso de antes?? ellos, usaban una red de pcs y la primera ip era 192.168.0.2 y la ultima del grupo era la 192.168.0.254.... pues esa es la network range o rango de ips, **TODAS** las comprendidas entre la 192.168.0.2 a la .254. ok??? Esto es util para englobar un rango de ips sin excepciones para las comprendidas en el y no tener que estar una a una poniendo reglas.

- **Permit o allow**: permitir o consentir algo.

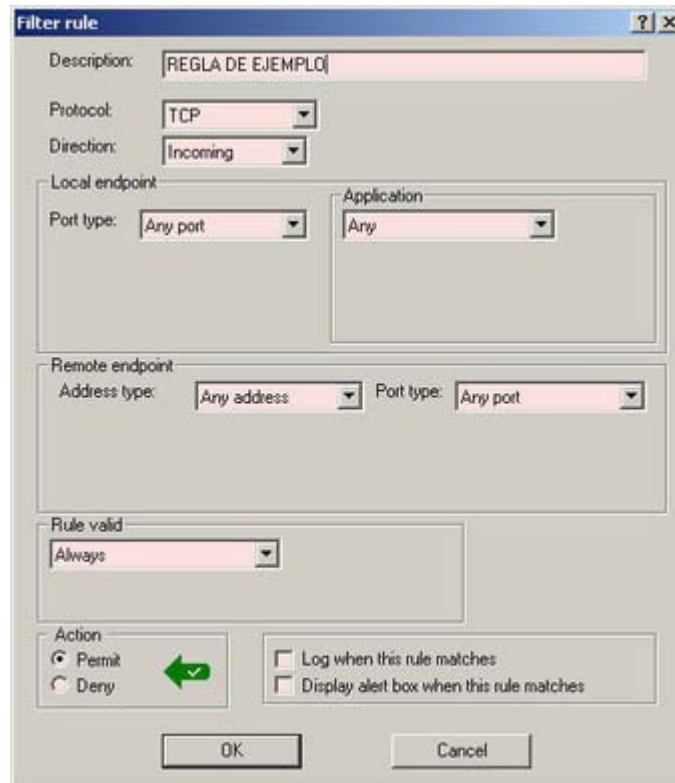
- **Deny**: denegar, impedir, bloquear.

- **Bill Gates**: muchas peliculas del anticristo han habido como damien la profecia, el exorcista, el fin de los dias, tcpa/palladium... pero este "xxxxxxx" es realmente quien nos ha dado a comer la manzanita y acabara con vaselina no quiero decir donde empujandonos por la espalda para

sentir muy de cerca su aliento en la nuca XDDDDDDDD.

## CREANDO REGLAS. COMO CREAR UNA REGLA.

Cuando nos encontramos en la ventana de **Filters Rules** vemos que abajo esta el ya explicado botoncito de **Add..** Este sirve para "añadir" y por lo tanto, de picarlo añadiremos en la ventana de reglas de filtrado o filters rules una nueva regla a las que ya kerio pone por defecto en nuestro sistema cuando se instala. Ahora, nosotros queremos empezar a crear reglas que se adapten a nuestras necesidades, de ahi que picamos como digo, Add... y vemos que nos aparece un cuadro como este



En **Description** pondremos lo que nos de la gana de forma que luego podamos identificar que regla hemos hecho. No tiene mas importancia el nombre que le pongamos mas que nos sirva para saber luego de que va esta regla o a que concierne.

En **Protocol** elegiremos que protocolo nos interesa para esta regla. Aqui podeis ver que estaba marcado el Tcp.

En **Direction** pondremos si la regla la vamos a aplicar para una aplicacion o un puerto de entrada ( **Incoming** ), si la regla sera para una aplicacion que va a salir ( **Outgoing** ) o esta regla afectara al trafico de entrada y salida ( **Both Directions** ).

En **Local Endpoint**, es la parte que afecta a nuestro sistema. En **port type** esta seleccionado "any port" dando a entender que sera para "cualquier" puerto local. Por eso, podremos definir un puerto cualquiera ( **any port** ), un puerto unico ( **single port** ), un rango de puertos ( **port/range** ) o lista de puertos ( **list of ports** ). Los puertos cuando es una lista o bien se pica uno y enter, se entra otro y enter... o se separan sin espacios con una comilla ",".

En **Application** podemos dejar el por defecto **any** ( que indicaria que no importa la

aplicacion/programa que este por esta regla implicado, sino que cualquiera, el que sea ) o bien, en **only selected below** picamos a browse y navegamos por los directorios hasta escoger la aplicacion a la que se le va a caer el pelo, jejejeje. Mejor dicho y bromas a parte, escogemos la aplicacion a la que le vamos a crear una regla para ella solita :-)

En **Remote Endpoint** podemos ya intuir que es el sitio remoto o de la conchinchina para la que estamos haciendo esta regla. Aqui, vamos a definir como va a trabajar kerio con el exterior para la regla de turno dandole la/s ip/s y el/los puerto/s.

En **Adress Type** diremos si esta regla va a afectar a una ip remota, si a un network range o rango de ips, si va a afectar a cualquier ip dejando el por defecto any adress... etc

En **Port Type** es lo mismo que antes, solo que ahora sera para el puerto de o de los host remotos.

En **Rule Valid** es mejor siempre dejar seleccionado **always** (siempre). Tambien podemos especificar la opcion de a intervalos de tiempo. Al hacer esto, se nos abran las opciones para definir los dias/horas y diremos a kerio en que intervalos de tiempo nos interesa que esta regla se cumpla.

En **Action** esta claro... o permitimos (**permit**) o denegamos (**deny**).

Y por ultimo, en las dos casillas de la derecha vemos las opciones de hacer que kerio escriba en el archivo log lo que suceda a partir de ahora con esta regla (log when this rule matches) y/o que encima nos muestre una ventanita de alerta si picamos la 2ª casilla de "Display alert box.....".

Cuando hayamos rellenado los campos especificando el protocolo, la direccion si es de entrada, salida o en ambas (both). Si la regla es para cualquier aplicacion o para una en concreto. Si es para un puerto o puertos locales o para cualquiera. Si es para una ip remota concreta, para unas ips de un rango determinado, si para cualquier ip remota... Si es para un puerto remoto o para algun tipo o lista de puertos.... Pues cuando hayamos configurado todos estos parametros, deberemos elegir si permitimos o denegamos logicamente. le damos a ok, aplicamos luego en la ventana de Filters Rules y ya tenemos nuestra regla hecha.

Ahora es muy importante saber algo sobre kerio. Si mirais la imagen de **Filters Rules** que esta en este manual, vereis un par de "flechitas" a la derecha. Estas flechas sirven para subir una regla hacia arriba o hacia abajo. Y para que carajo hay que moverlas se puede preguntar alguien. Muy simple, esto es como la vida compi, la regla de arriba vale mas que la de abajo. Como tu jefe, como tiene una posicion en la vida superior que la tuya, manda mas que tu. Sencillo no?? jeje.

Entonces la posicion de las reglas esten arriba o abajo **NO** importa **SIEMPRE Y CUANDO** dos, tres o mas reglas **NO SE CONTRADIGAN UNAS CON OTRAS.**

### **SIGUIENDO UN EJEMPLO DE REGLAS CONTRADICTORIAS.**

Por ejemplo, si yo creo una regla como esta para que mi programa PEPE v.1.3 pueda salir a internet donde le de la puñetera gana:

**Regla 1 que permite a pepe v.1.3 ir donde le de la gana**

**tcp**

**outgoing**

**local port:** any **local application:** c:\archivos.....\pepe\pepe.exe

**remote port:** any **remote adress:** any

**PERMITIR**

**PERO!!!** no me interesa que vaya a conectar con el pc de la tonta de mi novia pongamos el caso XDDDDDD.... debere **POR ENCIMA DE ESTA** poner otra regla para que **impida** que mi pepe.exe comunique con la ip del pc de mi novia....

### **Regla 2 que impide SOLAMENTE que pepe v.1.3 comunique con la ip de mi novia**

**tcp**

**outgoing**

**local port:** any port **local application:** c:\archivos.....\pepe\pepe.exe

**remote port:** any port **remote adress:** single ip = ip de mi novia

**DENEGAR**

Asi pues, cuando dos reglas se contradicen y una de ellas especifica algo, SIEMPRE por encima la que especifica como es el caso de la regla 2 y la Generica, SIEMPRE por debajo. Asi pues, en este caso de pepe.exe vemos que el JEFE que aqui manda para pepe es la regla 2, ya que nos interesa que pepe.exe salga donde quiera MENOS al pc de la novia. De poner la regla dos por debajo, pepe.exe iria tambien si le da la gana al pc de la novia logicamente y no estaríamos haciendo lo que aqui se pretende, que es permitir el acceso a la red de un programa como en este caso excepto a una ip, la de la novia.

Y si queremos estar seguros que no va a comunicar jamas encima la pelmaza la novia con mi pc sea la aplicacion que sea porque me tiene rayado y frito.... xDDD, haríamos esta regla:

### **Regla para ser invisible total a mi novia... ex-novia a este paso ;-p**

**protocolo:** any

**direccion:** both directions

**remote adress:** la de ip de mi novia

**DENEGAR**

Como podreis ver en vuestro kerio, si no selecciona un protocolo concreto como tcp, udp o icmp, se le dara a entender que puede ser "cualquiera" asi que kerio pasa de nuestro aspecto local y solo pregunta ip remota. Y esa ip remota no nos podra ni dar los buenas dias. La dejaremos total y absolutamente incomunicada con nuestro sistema.

### **MAS EJEMPLOS DE REGLAS**

Esta ya es un caso de regla real para aplicar al inutil del messenger. Con este par de reglas haremos algo muy chulo, podremos hacer que inicie sesion pero impediremos que nadie, ni nosotros mismos, podamos enviar/recibir archivitos y fotitos asi, como impediremos que messenger pueda conectar con mas ips que las de inicio de sesion. Osea, solo chatear y correo... ni netmeeting a traves de messenger, ni conferencias de voz ni leches. jejejeje. Solo chatear, correo y se acabo, hasta el banner de publi del mssger se jodera y no nos aparecera. XDD

### **Regla para permitir a mssger abrir sesion, chatting y mailing**

**protocolo:** tcp

**direccion:** outgoing

**local ports:** port/range del 1030 al 14000 **local application:** c:\.....\messger.exe

**remote port:** single port 1863 **remote ip:** network range de la ip 64.4.12.1 a la 64.4.13.254

**PERMITIR**

Con esta regla ya hemos avanzado un poco especificando puertos y rangos. En puertos locales ya especificamos que usaremos un rango comprendido entre el puerto 1030 al 14000. En el puerto remoto tambien concretamos que solo podra conectar al puerto 1863 y como ip remota tambien estrechamos el lazo dando un rango de servidores micro\$oft cuyas ips quedaran comprendidas en esas dos subredes de ips. De la x.x.12.1 a la x.x.13.254.

Pero ahora, y por debajo de esta (pues hemos dicho que la que especifique cuando dos o mas reglas se contradigan, debe ser la primera de su grupo), haremos otra regla para que kerio no nos ande preguntando:

- Oyeeee.... que mira..... que el mssger intenta ir aaaaaa..... y ahora intenta hacer estooooo queeeeeee..... le dejamos o no le dejamossss????

Pues precisamente para que kerio sepa que no puede hacer otra cosa mas que lo especificado en la regla anterior, creamos un generica que denegara cualquier intento de conexion de mssger o de alguien, hacia nuestro messger.

### **Regla para que mssger quede aislado a excepcion de iniciar sesion y punto**

**protocolo:** tcp/udp

**direction:** both direcciones

**local port:** any **application local:** el puto messenger

**remote port:** any **remote ip:** any

**DENEGAR**

Con esta regla, al quedar situada debajo de la anterior que hicimos, impedira que a parte de iniciar sesion como quedo especificado anteriormente, mssger.exe pueda hacer nada de nada. Es mas, al elegir el tcp mas el udp en ambos sentidos, hacia y desde cualquier puerto o ip remota hemos logrado aislar un programa el cual, solo puede conectar a una ip y puerto. Ahi se le acaba el chollo al colega del mssger. XDDDD

En el caso que algun dia queramos recibir un archivo via messenger o hacer netmeeting conectando por messenger, pues esta segunda regla deberemos de o bien, despicala de la casilla de verificacion que sale al crear una regla, o bien, darle a permitir en lugar de denegar si no queremos que nos ande kerio preguntando ahora. Eso si, en cuanto se acabe lo que se tenga que hacer, es preferible volver a ponerla en denegar.

### **UN ULTIMO EJEMPLO HABLANDO DE MSSGER.**

Pues ahora, pongamos que **SI** vamos a dejar siempre siempre, las dos reglas de arriba para que el mssger. solo pueda iniciar sesion (chat y correo), sin que nadie pueda ponerse en contacto con el ni este, con nadie pero.... PERO, nos interesa que solamente la tonta de la exnovia con la que ya he hecho las paces, pueda enviarme fotitos en ... ejem. para alegrarme los ojos.

Haremos una tercera regla. Esta debe quedar por encima siempre de la generica de denegacion como en este caso. Entonces, tanto dara que quede en primer como en segundo lugar pero jamas logicamente, por debajo de la generica pues quedaria nula.

### **Regla para que mssger. solo pueda conectar con la ip de la .... novia**

**protocolo:** tcp

**direccion:** both direcciones

**local port:** port/range 1030 al 14000 **application local:** mssger logicamente

**remote port:** any **remote adress:** single ip = la ip de la novia

**PERMITIR**

Con esta regla, permitimos que msger. pueda establecer conexiones por el protocolo tcp a la ip de nuestra novia, desde un puerto local comprendido entre el 1030 al 14000 a cualquier puerto de la ip de la misma

Lo interesante para no andar siempre tocando los filtros, es que si SOLO intercambiamos ficheros o hacemos comunicaciones de voz por micro con 3 o 4 personas, añadir una regla por ip remota y por ultimo la generica, ya que si eligieramos un remote network range incluiriamos en el

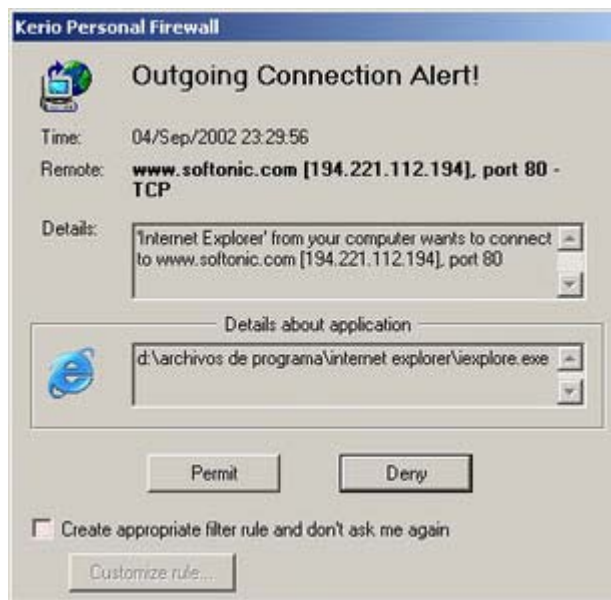
saco todas las ips desde la de un colega hasta varias miles mas al llegar a la ultima ip. Esto nunca se debe hacer.

## SIGAMOS CON MAS EJEMPLOS PRACTICOS EXPLICATIVOS.

Quiero hacer constancia que es imposible crear este manual con reglas concretas para cualquier usuario. El mismo usuario debe ser el unico responsable final de la configuracion de su cortafuegos. Por eso, seguire poniendo unos ejemplos mas antes de dar por finalizado este manual con los consejos finales.

Como ya hemos viendo hasta ahora, las reglas asi como el funcionamiento que nuestro kerio tendra a raiz de las mismas sera basado en lo bien o mal que estas esten definidas. Una configuracion demasiado estricta puede tener efectos negativos en cuanto a la viabilidad y fluidez del propio sistema en la red, asi como una configuracion con parametros pocos establecidos puede dar lugar a que aplicaciones locales como usuarios remotos, puedan tener mas permisos que lo que interesa.

Ahora, vamos a suponer que acabamos de instalar kerio, abrimos el navegador y nos aparece la primera ventanita de turno con la alerta de "outgoing conection.... bla bla". Como definimos las reglas?? Para empezar, cada vez que se nos abre una ventana de alerta, kerio nos esta indicando que algun tipo de conexion ha sido detectada y por lo tanto, al no existir ningun filtro para ese tipo de conexion, nos pregunta que debe hacer. En la ventanita de turno...



podemos ver hay un intento de conexion de nuestro sistema hacia la red. Nos indica la ruta de la aplicacion que atenta a salir fuera (outgoing) c:\archivos programa\internet explorer\iexplorer.exe, nos dice hacia donde lo intenta (www.softonic.com y la ip:puerto remotos) y por lo tanto, si lo permitimos o denegamos. Bien, si tan solo denegamos o permitimos, ira haciendonos la misma pregunta una e infinitas veces. En el caso que piquemos la casilla de "**Create appropriate filter....**" (traducido seria que cree una regla adecuada y no me preguntes mas), dicha regla se basara en la decision que ahora tomemos.... si permitimos y hemos picado dicha casilla, lo permitira siempre y si lo denegamos, lo denegara siempre. Pero, tal vez esto no sea lo mas adecuado aunque si lo mas comodo, ya que tal vez deseemos una regla generica para iexplorer **aunque** al mismo tiempo necesitaríamos o nos iria bien una especifica (ya sabeis, las especificas siempre por encima de las genericas) concretando algunos detalles.

En el supuesto que piquemos la casilla de que no me preguntes mas... y aceptemos picando a Permit, esta es la regla que aparecera en nuestra ventana de **Filter Rules** en ultima posicion de todas:

#### **Regla Generica para iexplorer**

**tcp**

**outgoing**

**local port: any application local: iexplorer.exe**

**remote port: any remote adress: any**

**PERMITIR**

Entonces, ya no nos preguntara mas, pues de momento solo existe esta regla que acabamos de crear "generica" sobre iexplorer en la cual como vemos arriba, permite desde cualquier puerto local, a cualquier ip:puerto remoto en el protocolo tcp.

Por ello, vamos a crear una regla especifica ( ojo!! pero hipotetica ein?? ). Pues bien, pongamos un ejemplo por el cual nosotros compartimos el pc con la novia y como no queremos que navegue por segun que web del Brad Pit que para tio gueno ya estamos nosotros aqui, entonces haremos una especifica y cuando este acabada la pondremos por encima siempre de la generica que hemos hecho:

#### **Regla Especifica para iexplorer- negar una web del braspit**

**tcp**

**outgoing**

**local port: any application local: iexplorer.exe**

**remote port: 80 remote adress: single ip y ponemos la ip de la pagina web del brasspit**

**DENEGAR**

jejeje, con esto, si hemos puesto contraseña a nuestro kerio para la administracion, acabamos de putear a la novia pero bien, pues kerio impedira que entre en esa web XDD. Pero, alguno se puede preguntar, y como coj... se yo la ip de la web??? Pues facil. Si recuerdas al principio de esta guia, estudiamos la ventana de monitorizacion asi que nada mas facil que para saber la ip de una pagina, que justamente abrirla y mirar la ventana de monitorizacion a ver la ip remota a la que se encuentre conectado en ese momento iexplorer. Recordad, que podemos obtener en la monitorizacion de kerio los datos segun los elijamos en la pestaña **Settings** de la misma ventana.

Sobre la opcion antes de permitir o negar cuando nos salta la ventana de alarma de turno sobre **Customize Rule** es interesante a tenerla en cuenta. Al picarla previamente a decir que si o no, vemos que en la opcion central esta la de decirle a kerio si solo para esa ip o dejarla como por defecto, any. Asi mismo, para los puertos locales y remotos que por defecto estan en any.

Yo siempre aconsejo por lo pronto de dejarlo en any los puertos, si bien la ip se puede concretar en ese instante e ir haciendo otras reglas nuevas a medidas que salten las ventanas de alerta para ir creando y perfeccionando las mismas concernientes a una aplicacion. Ojo, porque aun habiendo puesto como ejemplo iexplorer, el pretender crear reglas extrictas para ie seria de locos. Como para cualquier navegador que usemos a parte, sea mozilla, kmeleon, opera... por ello, lo mejor en el caso del navegador es dejar la regla generica puesta amen, de las especificas que estimemos oportuno crear.

#### **MAS EJEMPLOS.**

Ahora que con el ejemplo anterior hemos visto el tema de las ventanas de alerta, asi como se supone que ya se entiende que es una regla generica y una especifica, se debe aprender a hacer especificas, cosa realmente muy util.

Para empezar, pongamonos en el pellejo de un programa cualquiera. Lo instalamos y al lanzarlo aparece la tipica ventana de alerta de kerio con outgoing conecction alert!!. Bueno, suponemos que hemos lanzado el programa y joder.... que coño hace saliendo a internet el mismo programa?? Tal vez, este tenga por defecto la opcion de buscar actualizacion cada vez que se ejecute y claro, kerio lo engancha por los webOS ya que no hay regla alguna que diga que el programita de marras puede salir a campar por las buenas. Entonces, por lo pronto negamos y punto. Ahora, lo suyo es mirar la configuracion del programa a ver como esta por defecto. Si por casualidad vieramos esa pestaña picada que dice: buscar actualizacion en cada inicio, ya sabemos que intentaba hacer este canalla saliendo a la red, pero si no vemos nada de eso por mas que miramos, tendremos que sospechar que el programita lleva alguna clase de modulo que conecta con su web para facilitar datos nuestros como que somos un nuevo usuario de su software. Esto, no es buena idea para nada y maximo, si usamos soft ilegal, crackeado, pirateado... etc. Asi, que diremos a kerio que al listo del programa en cuestion, le pille del cuello con la regla de turno:

### Programa que va de listo, regla generica

tcp/udp

outgoing

local puerto: any aplicacion: el programita

remote puerto: any remote ip: any

**DENEGAR**

Esta es una generica para este programa. Sin embargo, tal vez queramos que se conecte a una sola ip con una submascara de red concreta como 255.0.0.0, a unos puertos remotos concretos que seran para el ejemplo, los 3000, 4000 y 5000, y solo podra conectar ese programa tanto si esta ejecutado como si no, los lunes y los martes desde las 18 horas a las 20 horas. la regla seria asi:

### Programa de turno, regla especifica

tcp/udp

outgoing

local puerto: any aplicacion: el programita

remote puerto: list of ports 3000,4000,5000

remote ip: network/mask ip y la mascara 255.0.0.0 debajo

**PERMITIR**

**PERO!!!!!!!** para que cumpla el horario y dias en los que esta regla especifica en **Rule Valid** en la que por defecto aparece **Always** ahora pondremos **In this interval only** y como vemos en la foto, tan solo nos cabe picar las casillas de los dias y poner la hora a la que la regla tomara efecto y a la hora que acabara la validez de la regla.



Ahora y como ultimo ejemplo hablare un poquito sobre el protocolo icmp, el cual sirve para comunicaciones de comprobacion entre varios host en la red. Se suele usar mucho para establecer distancias, tiempos y todo tipo de comprobacion entre dos host. Nosotros, solo vamos a tener presente de este protocolo icmp, el (8) y el (0), tambien conocidos como ping y pong, que no es precisamente el juego de las raquetas y la pelotita :-)

El ping lo hace nuestro sistema cada 2x3 a otros host para verificar si estan o no estan vivos por ahi, en algun lugar de la red. Al igual que otros pcs pueden hacernos a nosotros un ping o icmp (8) de salida para que a nosotros nos llegue ese ping como un "packet icmp 8 incoming alert!!".

De no negar los pings que nos hagan, nuestro sistema cada vez que un host remoto nos haga ping, le devolvera ping o "icmp (0) outgoing".

Es bueno o es malo esto?? Particularmente he de decir que no me hace gracia que alguien sepa si mi sistema esta o no esta conectado. Entonces, yo siempre tengo una regla creada para tal efecto en la que niego cualquier ping que me hagan sea quien sea venga de donde venga...

**Regla para negar los pings o icmps (8)**  
**protocolo icmp (8)**  
**incoming**  
**remote ip: any**  
**DENEGAR**

Tambien en plan ya masoca, jjejeje, he hecho otra para denegar por si las moscas, los pongs que desee enviar mi sistema aun teniendo denegado el icmp (8) de entrada que llamare ping a partir de ahora,

**Regla para negar el la respuesta a ping, que es pong o tambien, icmp (0)**  
**protocolo icmp (0)**  
**outgoing**  
**remote ip: any**  
**DENEGAR**

Ea, a partir de ahora ya nos pueden hacer pings que kerio tal como les llegue tal como se la sopla. Hubo un tiempo y aun hoy algunos caen con esto, en que si nos hacian un ping muy seguido con grandes packets (paquetes) de datos nos podian hacer colgar la conexion y el propio sistema, ya que a cada ping que un usuario malintencionado nos hacia desde su sistema, el tonto del nuestro respondia pong... y ping/pong hasta que de decir pong nuestro sistema acababa agilipollado... traduzcase a pantallazo azul y/o cuelgue de conexion/del equipo. Para esta ahora kerio, con estos filtros no habra problemas

Curiosamente, lo que SI nos interesa a nosotros es poder hacer ping y recibir los pong de otros. Entonces, debemos crear un par de reglas para esto en las que le diremos a kerio que SI permita el icmp (8) de salida y el icmp (0) de entrada. ok?? ya ni pongo ejemplos que es facil :-)

Espero que estos ejemplos hayan servido para conocer las virguerias a las que podemos llegar configurando kerio en nuestro sistema :-). El limite solo lo pones tu y tu capacidad de observar los logs y estudiar el comportamiento de tu sistema, aplicaciones, etc para hacer reglas tan paranoicas aunque totalmente competentes y funcionales, que cualquier lamer o aprendiz de hacker por muy puesto que vaya por la vida, si se topa con un kerio **bien** configurado, ya puede empezar a sudar tinta para penetrar en el sistema.

Kerio no tiene bugs conocidos y las alarmas y falsos cuentos que hay por ahi sobre las vulnerabilidades de kerio como cortafuegos mas bien parece cosa de la puta envidia y el alarmismo descarriado de otras casas de software que ven como sus productos no tienen ni el potencial ni la flexibilidad de este cortafuegos que de una realidad demostrable. Esta claro que si

nos ponemos a demostrar que un soft es inseguro, podremos demostrar con días y panes de estudio bugs en los mismos sistemas linux que teóricamente tan seguros son. Todo es cuestión de quien se ponga a buscar el bug y sepa encontrarlo. Por si alguien no sabe que es un bug, se conoce así por un fallo de programación en un programa, el cual repercute tanto en la seguridad del mismo como en su estabilidad.

## **FINALIZANDO EL MANUAL.**

Creo que tal y como me enrollado con ejemplos prácticos y teóricos en este manual, cualquiera que lo haya leído atentamente está más que preparado en cuanto a la configuración de kerio respecta, para ponerse manos a la obra y hacerse sus propias reglas a gusto según el software que tenga instalado y las necesidades de este de salir a la red, o de la red entrar al propio sistema.

Esta claro que en ningún momento me voy a emparanoiar explicando que es un puerto, una ip, una máscara subred o un protocolo con pelos y señales o a poner 1000 reglas de ejemplo para cada uno de los miles de casos que se pueden dar con el guindos pululando por la red. Esta será **TU** faena y **TU** responsabilidad aprender por ti mismo a hacerlo bien. Yo por mi parte he de decir que al moderar un foro en compañía de mi amigo Dvdrw, he creído conveniente crear esta guía para así y de una vez por todas, no andar a medias tintas repetiendome cuando alguien pregunta sobre kerio. Y es de entender, pues kerio necesita para su entendimiento y configuración de algo que no todos a veces tienen.... paciencia, lógica y comprensión.

Ahora debes de saber ligeramente que es un protocolo, que es un puerto, que es el cortafuegos, que función hace en el sistema... Creo que ahora solo queda de paciencia, tiempo y de aquí a unos días y mientras más tiempo pases usando kerio mejor, podrás verdaderamente estar tranquilo no, tranquilísimo navegando y estableciendo conexiones remotas ya que sabrás como hacer para que kerio te controle el cotarro.

## **CONSEJOS.**

- Es muy importante el leer algo sobre los puertos y servicios más usuales que emplea el sistema que tengamos. No son las mismas necesidades las de un guindos 98 que las de un guindos 2000, por no hablar de ese enjendro que micro\$oft se emperrea en llamar Sistema Operativo.. guindos XP. El que llamen sistema a eso, es insultar a un linux o a un win2000 pro, sinceramente. Los puertos más importantes a cubrir en un windows win9x/2000 o sea, a negar el acceso desde cualquier ip siempre y cuando no estemos formando parte de una red o necesitemos tener abierto por razones X serán pues para tcp/udp---->

21: acceso a nuestro sistema por ftp

22: secure shell

23: conexión remota a telnet

25: smtp. Si no tenemos un servidor (un cliente sería outlook) de correo este puerto hay que cerrarlo.

80: conexión a nuestro navegador.

113: solo es necesario para irc, para que el irc server vea nuestro ident. Crear reglas específicas para servidores irc y cerrar el puerto a cualquier otro host remoto. Usado por el troyano kazimas.

137, 138 y 139: conexiones remotas a netbios. Si no estamos compartiendo recursos de red, crear reglas para estos puertos y denegar cualquier acceso a ellos de un host remoto.

161: snmp o simple network management protocol. Es mejor tenerlo cerrado para evitar envío de packets a este puerto por el cual, se pueden sacar vulnerabilidades de nuestro sistema como padecer ataques. Hay muchas hacktools especializadas en este puerto. Mas propio por eso en unix.

445: o microsoft ds. Este es el puerto de servicios por excelencia entre sistemas win2000/xp. Es muy importante que si usas estos, lo tengas siempre cerrado por defecto.

Por cerrar puertos los puedes cerrar todos :-), pero lo mas aconsejable es observar los servicios que tengamos establecidos en nuestro sistema, como podria ser un escanner antivirus de mail entrante al pop3, puerto 110, y hacer unas reglas para este servicio y puerto. En cuanto a troyanos, hay tantos puertos a cerrar que lo mejor es poner los puertos de los mas usuales como el 1433,1434,5000,12345,27374,31332,31120..... para esto, una regla generica en incoming tcp/udp a list port y estos tal como estan ahí, separados por coma o entre puerto y puerto, enter.

Agrego una direccion de puertos comunmente usados por troyanos--->

<http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html>

- En cuanto a las reglas, es muy aconsejable el marcar estas por las que tengamos interes en seguir su desarrollo, con las casillas **de log cuando la regla se cumpla** y **mostrar ventana cuando esta regla se cumpla**. Con esto, podemos ver en todo momento mientras estamos conectados que patrones de conducta sigue un programa, un un puerto de nuestro equipo, o una ip rara que se emperra en scannearnos los puertos del sistema en busca de alguno abierto.

- JAMAS optes porque no sepas como hacer una regla/s para una aplicacion concreta que necesite salir a la red, por quitar kerio como aplicacion de fondo. De acuerdo, ahora esa aplicacion podra salir y entrar a su libre antojo, pero tambien el resto de servicios y aplicaciones locales, asi como cualquier ip podra intentar impunemente establecer conexion con nuestro sistema. Tenedlo muy presente.

- Si alguna vez os pasa que en diferentes dias/horarios y mirando el log veis que hay constancia de alertas sobre una ip concreta, debereis fijaros que intentaba hacer... si queria entrar por un puerto concreto, si los escaneaba todos, que protocolo usaba... etc. y usando una pagina como esta--->

<http://network-tools.com/>

podreis averiguar el isp de esa ip y algun dato extra. De seguir observando intentos persistentes y reiterados asi como demasiados obvios de intento de intrusion, debereis dar parte a vuestro isp via email con acuse de recibo, adjuntando copia del archivo log de kerio con vuestros datos de cliente y datos personales. (no hace falta que pongais tambien el cumple de la novia y el numero cta. cte. del banco XDD). Vuestro isp si es como debe ser (telefonica en mi caso tardo 5 minutos en darme una respuesta via telefonica, 6 en ofrecerse a las 6 de mañana un tecnico pasar por casa y una semana mas tarde me llamaban de nuevo para asegurarse que todo estaba ok), debiera ponerse en contacto con vosotros y tomar parte en el asunto. Segun el grado de profesionalidad que noteis en un caso como este, si veis que no os atienden como debieran, podeis mandarlos a la mierda sin mas miramientos y buscaros otro.

- No penseis que hacer reglas concretas o paranoicas esta nunca de mas. Al que le gusten los pasatiempos como sopas de letras, crucigramas, o la estrategia militar, disfrutara como un loco currandose reglas en plan profesional. Es justo lo que me pasa a mi, jejeje.

- NO useis windows XP, NO useis outlook con plena confianza. Outlook es medalla de oro y record olimpico habiendo otorgado las mayores infecciones de gusanos del mundo por mail. Hay gusanos especializados y diseñados para joderte vivo si te llegan a outlook, como el caso de la saga de virii Kletz.

- Ultimo consejo, pensad siempre que kerio NO esta bien configurado aun teniendolo todo de p.m. Asi, siempre estareis desarrollando algo que a la mayoría de los chatters se les acorta... el cerebro. jejeejeje, no chateis demasiado que no es bueno. Leer es el mejor deporte para el coco.

## **NOTA FINAL.**

Si en algun momento he metido un gambazo por algun lado no ha sido mi intencion. Si he cometido alguna falta de ortografia perdon, que me da vicio esto de aporrear teclas y mi coco va mas rapido que mis manos. Si alguien se siente ofendido por decir que otros cortafuegos son kaka comparados con kerio, o que outlook es una mierda, que Bill Gay es marica, que micro\$oft son ladrones o que windows XP es una basura..... lo siento, la verdad jode, pero curte.

Durante el manual he puesto ejemplos teoricos excepto alguno como los de icmp, mssger y explorer regla generica. Si alguno se llama Pepe de los que lea este manual espero que no se haya sentido ofendido cuando he usado el nombre "pepe" para citar un programa cualquiera. Si alguna ex-novia mia ve mi foto y sabe quien soy por no decir de los ejemplos a los que he hecho referencia y terminos a los que me he referido... pues .... cariño, no te sientas aludida que mis ex-novias tu ya sabes que han sido muchas y lo mismo no me inspiraba en ti, sino en otras y he de decir que ahora estoy libre de nuevo y .... si te has teñido rubia o lo eres ..... jum.  
XDDDDDD

Bueno, fuera de coñas, ahora si que acabo ya que son las tantas de la mañana y llevo ya horas escribiendo. Gracias por leer el manual si me has aguantado hasta este punto y nos vemos por los foros.

**SALUDOS.**

**ZORTH**