BREVE INTRODUCCIÓN A IPSEC

La seguridad ha sido, desde siempre, el gran caballo de batalla para los administradores de sistemas. Dentro de las múltiples soluciones que podemos implementar en nuestra instalación nos centraremos hoy en IPSEC.

IPSEC no es más que el envío de paquetes de información cifrados a través del protocolo TCP/IP estándar. Es decir, la información viaja codificada entre dos o más equipos. Esto tiene una repercusión inmediata en nuestra red: aumenta el tráfico de red y el rendimiento del procesador cae por la carga extra que supone el cifrado. Pero es una forma muy efectiva de mejorar la seguridad.

2 Modos:

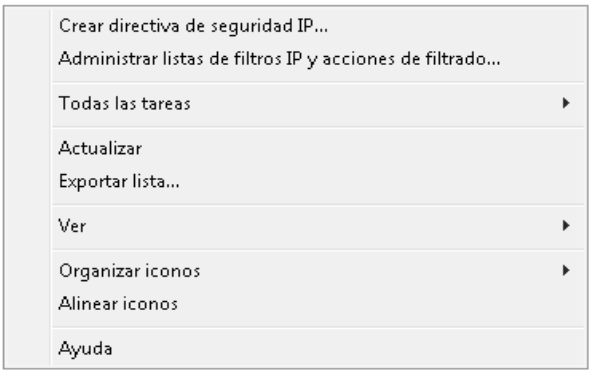
- Transporte: Entre dos ordenadores con IPSEC.
- Túnel: Entre dos firewall.

Los protocolos que emplea IPSEC son:

- AH "Autentication Header" que se encarga de la autenticación.
- ESP "Encapsulation Security Payload" para la confidencialidad.
- IKE "Internet Key Exchange" para el negociado.

A nivel práctico podemos acceder a las directivas IPSEC a través de la consola de Windows (Inicio – Ejecutar – MMC) agregando el complemento Directivas de Seguridad IP.

Botón derecho y seleccionamos Crear directiva de seguridad IP...

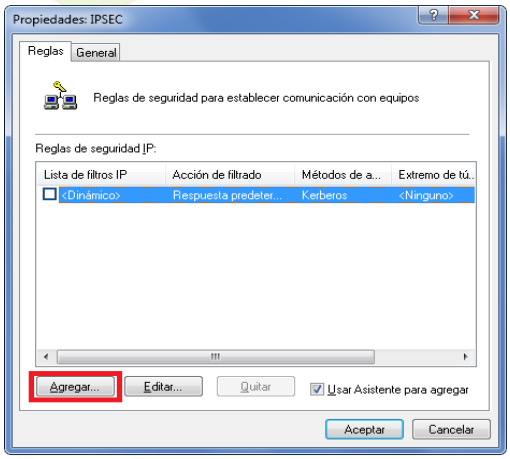


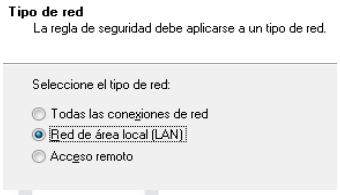
Aparecerá un sencillo asistente.

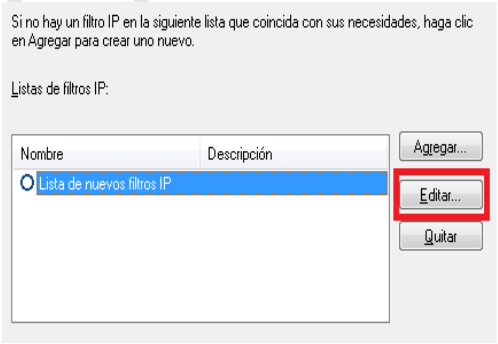
Indicar un nombre para la directiva, por ejemplo "IPSEC" y **no** marcar la regla de respuesta predeterminada.

BREVE INTRODUCCIÓN A IPSEC

En el paso anterior hemos creado una directiva nueva llamada IPSEC, ahora agregaremos algunas reglas pulsando en Agregar. Fijarse que "Dinámico" no está marcado, si lo está desmarcarlo.







Lo que vamos a hacer es crear "Reglas" de filtrado dentro de nuestra directiva. Una directiva se compone de una o varias Reglas que nos permitirán filtrar las IPS, los puertos orígenes o de destino para el cifrado.

Empezaremos por no especificar un túnel.

En tipo de red, podemos elegir qué interfaz es la que vamos a securizar. Por ejemplo, vamos a elegir la interfaz LAN, aunque podríamos elegir acceso remoto y cifrar las conexiones con los usuarios de Remote Desktop.

Recordando siempre que cuando más cifremos más lento irá todo.

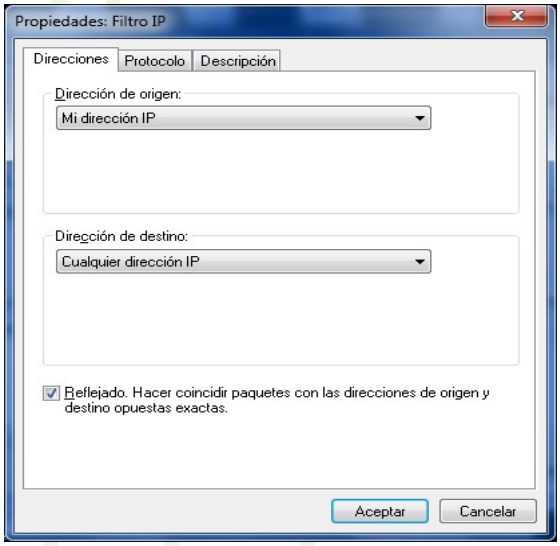
Ahora vamos con los filtros, clic sobre "Editar" en la pantalla de filtros IP. Vamos a configurar uno para el comando PING.

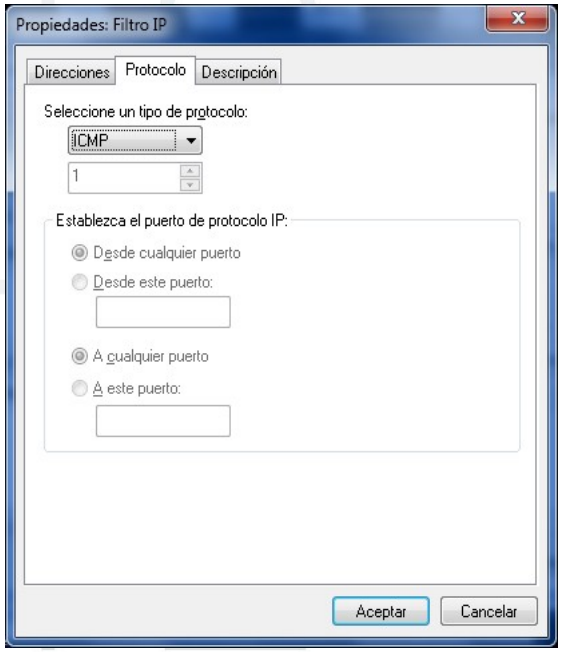
En el nombre de la lista de Filtros podemos poner "PING" para saber que eso es lo que vamos a filtrar.

Una lista de filtros IP hace las negociaciones de seguridad en función de una correspondencia con el origen, el destino y el tipo de tráfico IP. Este tipo de filtrado de paquetes IP permite a un administrador definir con precisión el tráfico IP que debe protegerse. Cada lista de filtros IP contiene uno o varios filtros, que definen las direcciones y los tipos de tráfico IP.

BREVE INTRODUCCIÓN A IPSEC

A continuación configuraremos las tres pestañas del filtro:
Direcciones Protocolo Descripción





Direcciones.

Como dirección de origen indicaremos "Mi dirección IP" y como dirección de destino "Cualquier dirección IP" o una IP conocida de otro equipo en la red sobre el que hagamos la prueba.

Protocolo.

El que hemos de usar en nuestro caso es ICMP para el ping, pero podríamos seleccionar TCP y entonces permitiría escoger, además, un puerto.

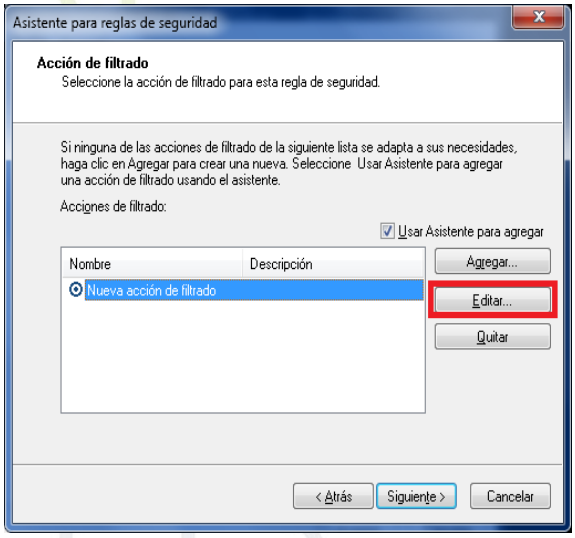
Descripción

Aquí pondremos una descripción de lo que hace el filtrado.

Con esto finaliza la edición de la regla de filtrado, pulsar Aceptar para volver a la pantalla anterior y pulsar siguiente.

BREVE INTRODUCCIÓN A IPSEC

Una acción de filtrado define los requisitos de seguridad para la transmisión de datos. Las acciones de filtrado pueden definirse al crear una directiva o antes de crearla. Las listas de filtros se encuentran disponibles para todas las directivas. Aparece una ya creada. Pulsar sobre "Editar"



Métodos de Seguridad.

Vemos que existen 3 posibilidades, permitir, bloquear o negociar.

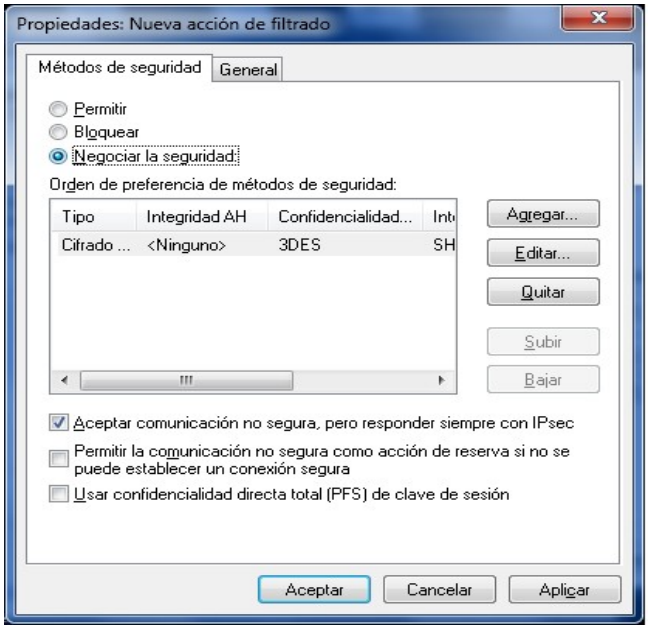
Permitir: Se permite el tráfico "tal cual" desde la regla de filtrado. Esto es útil para equipos no compatibles con IPSEC.

Bloquear: No se permite el tráfico indicado. Ideal para bloquear accesos desde equipos (IPS) no autorizados, en un rango etc.

Negociar la Seguridad: Aquí podremos establecer el nivel de negociado en protocolos de integridad, confidencialidad y cifrado.

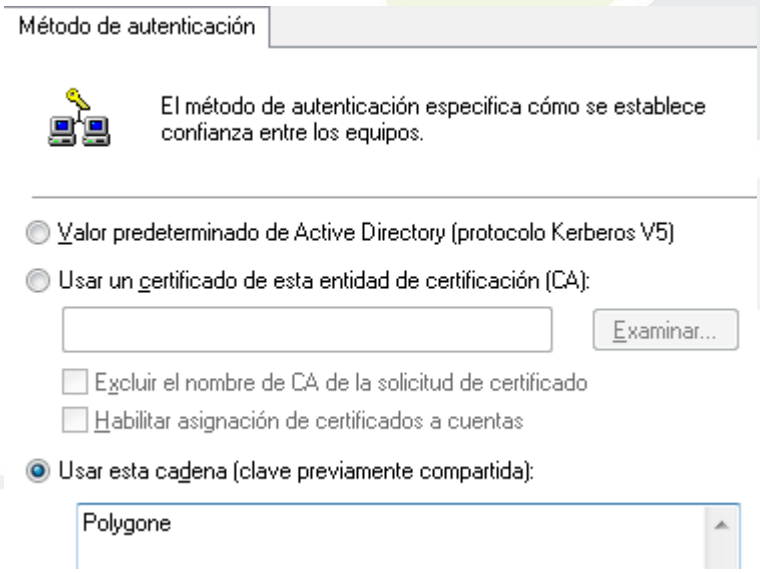
En "Agregar" y en la opción "Personalizar" de la pantalla que aparece, podemos indicar nuevas combinaciones de protocolos. Recordar que DES y MD5 son protocolos "NO SEGUROS".

Hay otra pestaña de General que nos permite cambiar el nombre de la acción de filtrado.



BREVE INTRODUCCIÓN A IPSEC

Los métodos de autenticación dependerán del escenario en que nos encontremos. Para nuestro ejemplo, suponiendo que no estamos en un dominio, vamos a emplear "Clave Previamente Compartida" Shared Key. Al seccionar esta opción escribiremos la "clave" de forma parecida al WIFI.



De esta forma, solo los equipos que tengan la misma clave y respondan a la regla de filtrado, podrán estar bajo IPSEC.

El último paso es "Asignar" la Directiva IPSEC para que funcione. Esto lo conseguimos con el botón derecho sobre el nombre de IPSEC y "Asignar".