

POLICIA FEDERAL ARGENTINA



**SUPERINTENDENCIA FEDERAL DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES**

Departamento CIBERSEGURIDAD

División SEGURIDAD INFORMÁTICA

**Bloqueo de IP a través del Firewall
ESET**



Procedimiento de bloqueo de IP

Tipo de Documento:

Informe

Versión: 1 / 2022

La siguiente representación es un ejemplo de como bloquear IP maliciosa haciendo uso de las políticas implementadas en la totalidad del parque informático administrado desde la consola ESET PROTECT a través de la creación de una regla en el FIREWALL.

- Localizar la política: ***Política utilizada en la actualidad***

➤ *Editar*

The screenshot shows the ESET PROTECT interface. On the left is a sidebar with various icons. A red box highlights the gear icon in the toolbar. The main area displays a list of policies under 'Políticas'. A red box highlights the 'Edit...' button for a specific policy entry. To the right, a detailed view of the selected policy is shown, titled 'POLÍTICA DEL PRODUCTO'. It lists several items, each with a status indicator (green checkmark) and a 'Editar...' button. The items include: ESET Endpoint for Windows, and ESET Full Disk Encryption.

- Configuración

➤ *Protección de red*

➤ *Firewall*

➤ *Avanzado (Reglas), Editar*

The screenshot shows the 'Editar política' (Edit Policy) screen in ESET PROTECT. The left sidebar has a red box around the 'Configuración' tab. The main panel shows the configuration for 'ESET Endpoint for Windows'. The 'PROTECCIÓN DE RED' section is expanded, with the 'Firewall' sub-section highlighted by a red box. The 'AVANZADO' section is also highlighted with a red box. Other sections visible include 'BÁSICO', 'SERVICIOS PERMITIDOS', 'PERFILES DE FIREWALL', 'DETECCIÓN DE MODIFICACIONES DE LA APLICACIÓN', and 'CONFIGURACIÓN DE MODO DE APRENDIZAJE'. On the right, there are several tabs for managing rules, each with a status indicator (green checkmark) and an 'Editar' button.



Procedimiento de bloqueo de IP

Tipo de Documento:

Informe

Versión: 1 / 2022

- Reglas de firewall (buscar **IP_BlackList_SOC**)
 - *Editar*
 - *Local*
 - *IP*

The screenshot shows the Windows Firewall Rule Editor. On the left, there's a sidebar with tabs: Básico, Configuración (which is selected), Asignar, and Resumen. In the main area, there's a title 'Reglas de firewall' and a sub-section 'Las reglas'. A 'Nombre' dropdown shows 'Denegar conexiones de red para rundll3.exe (SysWOW64)'. Below it, there are tabs for General, Local (which is selected), and Remoto. Under the Local tab, there's a 'Puerto' section with a dropdown set to 'IP'. A large text input field contains a list of IP addresses separated by commas and spaces. At the bottom of the dialog are buttons for Agregar, Editar, Quitar, Importar, Exportar, and Aceptar.

Cabe aclarar que se debe respetar una sintaxis, esto quiere decir que por ejemplo en la imagen anterior se ingreso IP's y luego de cada una de ellas se agrega una COMA (,) y un ESPACIO con excepción del último ingreso.

Lista de direcciones o subredes de IP. Se deben delimitar múltiples entradas con una coma.
Ejemplo: 192.168.1.5, 10.1.0.25-10.1.0.99,
10.1.0.0/255.255.0.0, 10.2.0.0/16, ::1, fe80::/64

A continuación, se puede visualizar la tarea realizada.

This screenshot shows the Windows Firewall Rule Editor after changes have been made. The 'Nombre' dropdown now shows 'IP_BlackList_SOC'. The 'Puerto' dropdown is still set to 'IP'. The main pane displays a table of rules. The first rule is 'Denegar conexiones de red para rundll3.exe (SysWOW64)', which has its 'Habilitado' checkbox checked. The second rule is 'IP_BlackList_SOC', also with its 'Habilitado' checkbox checked. Both rules have 'Cualquier perfil' selected for 'Protocolo' and 'Perfil'. The 'Acción' column shows 'Denegar Ambos' for the first rule and 'Denegar Entrante' for the second. The 'Dirección' column lists the blacklisted IP addresses. At the bottom, there are buttons for Agregar, Editar, Quitar, Copiar, and Aceptar.