Análisis de aplicación: Cortafuegos de la distribución IPCop

Este documento ha sido elaborado por el **Centro de Apoyo Tecnológico a Emprendedores** - bilib, www.bilib.es

Índice de contenido

DATOS TÉCNICOS

Nombre: Cortafuegos de la distribución IPCop
Versión: 2.0.4
Licencia: GPL v2
Idioma: Español
Web oficial: http://www.ipcop.org
Manual (inglés): http://www.ipcop.org/2.0.0/en/admin/html/firewall.html
Descripción básica: IPCop es una distribución GNU/Linux para servidores dedicada a funcionar como cortafuegos -aunque dispone de más funcionalidades-, configurable mediante acceso por interfaz web. Fue diseñada para su uso en oficinas domésticas y PYMEs.

FUNCIONALIDAD

• Soporte a cuatro tipos de interfaces

Ordenadas de mayor a menor nivel de confianza, éstas son:

- Verde: Red interna de confianza.
- Azul: Red inalámbrica de confianza media. Puede usarse como una Verde secundaria.
- Naranja: DMZ o zona desmilitarizada para los servidores accedidos desde Internet.
- Roja: Conexión a Internet.

• Filtrado de paquetes o cortafuegos

El cortafuegos de IPCop está **basado en IPTables**. IPTables [1] es un programa de línea de comandos usado para configurar el conjunto de reglas de filtrado de paquetes de los sistemas GNU/Linux. Este programa permite añadir, modificar y eliminar reglas de la configuración de filtrado establecida.

Pueden establecerse un conjunto de reglas para cada tipo de interfaz de los vistos anteriormente, puesto que cada interfaz tiene asociado un determinado nivel de confianza en función del tipo de tráfico al que están expuestas. Así, la más restringida sería la Roja y la menos, la Verde. En la descripción de las políticas de seguridad del cortafuegos [2] puede encontrase información detallada sobre este apartado.

Hay tres **políticas de acceso** para las interfaces, salvo excepciones - Naranja abierta o cerrada, Roja cerrada. Éstas son:

- Open: Acceso abierto a servicios de IPCop y cualquier otra interfaz.
- Half-open: Acceso abierto a servicios de IPCop.
- Closed: Acceso completamente cerrado a la interfaz. Si se necesita acceso a una interfaz con esta política, debe crearse una regla específica para dicho acceso.

Se dispone de dos **opciones de denegación de acceso**, seleccionables por el administrador para ser llevadas a cabo al descartar un paquete. Son las siguientes:

- Drop: Descarta un paquete entrante de manera “silenciosa”, es decir, deniega el acceso pero no informa acerca del bloqueo.
- Reject: Descarta un paquete entrante y envía de vuelta un paquete ICMP. Se recomienda no utilizar esta opción en la interfaz Roja (Internet), ya que se expone el sistema a un posible ataque de denegación de servicio, DoS.

El **filtro de direcciones** permite restringir el acceso a una interfaz Azul (WiFi), autorizando únicamente la conexión de los clientes cuyas direcciones estén activadas en la lista de filtrado, siempre dependiendo de la política de acceso establecida. Si esta funcionalidad no está habilitada, tendrán acceso a la interfaz todos los clientes habilitados según la política de acceso.

• **Otras funcionalidades de IPCop**

- Soporte a DHCP como cliente y como servidor.
- Cliente y servidor NTP.
- Soporte a VPN.
- Soporte Proxy para navegación web y direccionamiento DNS.
- Administración y configuración a través de interfaz web, con posibilidad de visualización de gráficas.

Fallos y/o carencias importantes

La configuración y administración del cortafuegos requiere de conocimientos medianamente avanzados, ya que los menús y opciones no son nada triviales por la complejidad de los conceptos de seguridad informática utilizados por un cortafuegos. Esto no es considerado un fallo o carencia de esta herramienta en particular, sino un inconveniente característico de herramientas de este tipo.

USABILIDAD

Diseño de la interfaz

La interfaz es muy sencilla en cuanto a diseño, cuidando más la completitud de los datos y la facilidad de acceso que el aspecto, es decir, es más útil que bonita. Los submenús están clasificados por pestañas y desplegables accesibles desde el menú superior de la página.

El diseño puede recordar a la interfaz de configuración remota de la mayoría de los enrutadores o routers, con la característica más común de las interfaces web: está basada en formularios. El uso de listas desplegables evita la sobrecarga memorística del usuario, haciendo prescindible la memorización de datos que el usuario no tiene por qué conocer.

Por último, la representación de los tipos de interfaces mediante colores hace más intuitiva la identificación de una interfaz con su tipo asociado. Además, estos colores van directamente asociados con el riesgo que se asume en cada uno de los tipos, siendo el color rojo para la de mayor riesgo y el verde para la de más confianza.

Facilidad de uso

Sin necesidad de centrarnos en este cortafuegos en particular, la administración y configuración de cualquier cortafuegos requiere de unos conocimientos más que básicos sobre seguridad informática.

Accesibilidad

Esta herramienta no dispone de herramientas de accesibilidad propias, siendo necesario recurrir a las incorporadas por el sistema operativo. Sin embargo, la representación que se hace de los datos mediante formularios facilita el uso de la interfaz con la ayuda de herramientas de tecnología asistida.

Plataformas disponibles

Este cortafuegos es un panel de gestión incorporado por la distribución IPCop. Su funcionalidad está basada en IPTables, incorporado en el framework Netfilter, disponible en todas las plataformas GNU/Linux.

Plugins

IPCop permite ampliar su funcionalidad mediante la inclusión de add-ons o plugins, además de dar la posibilidad a los usuarios de crear los suyos propios y empaquetarlos. Puede encontrarse más información en el catálogo de add-ons de la distribución [3].

RENDIMIENTO

Requisitos hardware

Sistema operativo: IPCop 2.0.4
Procesador: 486 o superior
Memoria RAM: 64 MB o superior
Espacio en disco: 512 MB o superior
Tarjeta Gráfica: No procede, se maneja por consola

Consumo de memoria

La distribución IPCop está preparada para funcionar en equipos con un mínimo de 64 MB de memoria RAM y 512 MB libres de espacio en disco, por lo que el consumo de memoria no es excesivo ni en el caso de la memoria principal ni en el de la memoria secundaria.

Velocidad de ejecución

La velocidad de ejecución y de uso es, en general, fluido. En la mayoría de los casos, la fluidez dependerá de las características y el estado de la red, al acceder mediante interfaz web desde un equipo externo.

DOCUMENTACIÓN

En la web del proyecto oficial de IPCop se puede encontrar una amplia documentación acerca del uso de las herramientas disponibles en la distribución. Esta información no está disponible en español, pero sí en inglés y alemán, además de francés e italiano para algunos de los documentos.

La página de documentación [4] que ofrece la comunidad del proyecto recoge gran variedad de documentos, incluyendo un manual de instalación, una guía de inicio rápido y un manual de administración y configuración. Además, existe documentación para desarrolladores [5], donde se describen las formas de contribuir al proyecto.

También se puede encontrar una sección de preguntas frecuentes (FAQ) [6] y una wiki [7] muy completa, en la que se incluye por ejemplo el procedimiento para migrar de IPCop v1.4 a IPCop v2.

COMUNIDAD

Número de usuarios

Según la página de IPCop en Sourceforge.net [8], el número de descargas de la imagen .iso de la distribución es de aproximadamente 8.000 en estos momentos, con más de 500 recomendaciones.

Foros y portales de ayuda

El usuario dispone de varias opciones para obtener ayuda: varias listas de correo (para usuarios, desarrolladores...), numerosos foros (en inglés, alemán, francés...) y la sección de preguntas frecuentes (FAQ).

Contribuciones

Se puede colaborar con el proyecto desarrollando add-ons o ayudando en las traducciones tanto de documentos como de la distribución. Cualquier usuario puede unirse a las listas de correo, responder a preguntas de otros usuarios, enviar informes y correcciones de errores y proponer nuevas características.

Frecuencia de versiones

La primera versión de IPCop de la que se conoce la fecha de publicación es la versión 1.2, publicada el 18 de Septiembre de 2003. Desde entonces, se han ido liberando numerosas versiones con las correspondientes correcciones y mejoras, hasta llegar a la 2.0.4, versión actual de la distribución.

REFERENCIAS

[1] - http://www.netfilter.org/projects/iptables/index.html

[2] - http://www.ipcop.org/2.0.0/en/admin/html/firewall.html

[3] - http://sourceforge.net/apps/trac/ipcop/wiki/Addons

[4] - http://sourceforge.net/apps/trac/ipcop/wiki/Documentation

[5] - http://www.ipcop.org/development.php

[6] - http://sourceforge.net/apps/mediawiki/ipcop/index.php?title=FAQ

[7] - http://sourceforge.net/apps/mediawiki/ipcop/index.php?title=Main_Page

[8] - http://sourceforge.net/projects/ipcop/