Análisis de aplicación: Cortafuegos de la distribución clearOS

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 clearOS
Versión: Community 6.2.0
Licencia: GPL v2
Idioma: Español
Web oficial: http://www.clearfoundation.com
Manual (inglés): http://www.clearfoundation.com/docs/howtos/start
Descripción básica: clearOS es una distribución GNU/Linux para servidores enfocada a pymes, que incluye la funcionalidad de cortafuegos entre varias otras. Es configurable mediante acceso por interfaz web. Puede instalarse en un servidor hardware, en una máquina virtual o en la nube.

FUNCIONALIDAD

• DMZ Firewall - Cortafuegos DMZ

Establecer una zona desmilitarizada (DMZ) en la red de la empresa puede aumentar considerablemente la seguridad de la misma. Una DMZ estará aislada de la red local (LAN) de la empresa, de forma que el tráfico desde el exterior pasa por esta zona y desde ésta a la LAN. Así, al establecer un filtrado en la DMZ, llegará a la LAN únicamente el tráfico exterior que supere dicho filtrado.

• Egress Firewall - Cortafuegos de salida

Así como se establecen reglas de filtrado en la entrada, también pueden especificarse para el tráfico de salida desde la LAN de la empresa. De esta manera, pueden bloquearse varios tipos de tráfico que tengan como origen la LAN y como destino una red externa.

• Definición manual de reglas

Pueden modificarse manualmente las reglas del cortafuegos [1] mediante consola, editando el fichero /etc/firewall con el editor vim, incluido en clearOS. Esta opción sólo es recomendable para usuarios expertos, por su dificultad y porque mediante la edición manual pueden producirse fallos inesperados y difíciles de detectar.

• Otras funcionalidades de clearOS

- Protección antivirus.
- Protección antiphising.
- Sistema de detección de intrusos.
- Sistema de prevención de intrusos.
- Servidor Proxy.
- Servidor MySQL.
- Servidor FTP.
- Servidor DNS.
- Servidor DHCP.
- ...

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.

Además, no se ha podido determinar si es posible establecer reglas de filtrado en los cortafuegos para el tráfico dentro de la LAN de la empresa.

USABILIDAD

Diseño de la interfaz

La interfaz, de diseño sencillo, está muy bien estructurada en cuanto a clasificación de aplicaciones disponibles en la distribución. Cada una de ellas aparece localizada en la sección correspondiente, sin realizarse esta clasificación en demasiadas secciones, lo cual podría dificultar al usuario la localización del acceso a las aplicaciones.

Estas secciones anteriormente comentadas pueden ser accedidas desde la barra superior o la barra lateral. En la barra superior, de cada sección aparece un menú desplegable con todas sus subsecciones cuando el usuario se detiene sobre ellas, pudiendo seleccionar la subsección a la que nos interese acceder. En la barra lateral, se pueden visualizar de forma estática todas las subsecciones de una sección concreta, desplegándola en forma de lista. Esta variedad en las formas de acceder a la información facilitan al usuario la orientación a través de la interfaz.

Las opciones de configuración se encuentran altamente detalladas mediante formularios, siendo posible elegir adecuadamente el valor de cada uno de los parámetros que influirá en el comportamiento del cortafuegos. Además, se proporcionan numerosas pistas que guiarán al usuario a través de la configuración.

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.

PORTABILIDAD / ADAPTABILIDAD

Plataformas disponibles

Este cortafuegos es un panel de gestión incorporado por la distribución clearOS. Su funcionalidad está basada en IPTables [2], incorporado en el framework Netfilter, disponible en todas las plataformas GNU/Linux.

Plugins

clearOS permite ampliar su funcionalidad mediante la instalación de aplicaciones adicionales accesibles desde el marketplace, además de dar la posibilidad a los usuarios de desarrollar las suyas propias.

RENDIMIENTO

Requisitos hardware

Sistema operativo: clearOS Community 6.2.0
Procesador: Desde 500 MHz hasta 3 GHz
Memoria RAM: Desde 512 MB hasta 2 GB
Espacio en disco: A partir de 1 GB
Tarjeta Gráfica: No procede, se maneja por consola/interfaz web

Los requisitos hardware específicos para CPU y RAM dependerán del número de usuarios que deba soportar clearOS. Puede encontrarse información detallada en el apartado de requisitos hardware de la web de clearOS [3].

Consumo de memoria

La distribución clearOS puede llegar a exigir de recursos de memoria medianamente altos, dependiendo de la funcionalidad a cumplir. Sin embargo, esto hace referencia al correcto funcionamiento de un conjunto de aplicaciones adicionales a la de cortafuegos, por lo que estas exigencias no son específicas para el cortafuegos de la distribución. Para funcionar únicamente como cortafuegos, los recursos necesarios serán mínimos ya que no debe soportar una gran carga.

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 de clearOS se puede encontrar documentación [4] acerca del uso de las herramientas de la distribución, disponible únicamente en inglés. La mayor parte de la información disponible es sobre instalación del producto, siendo mínima para la configuración. Esta documentación hace referencia a ClarkConnect, nombre con el que se conocía anteriormente a clearOS.

Además, existe documentación para desarrolladores [5], donde se describen las formas de contribuir al proyecto, por ejemplo, desarrollando aplicaciones o colaborando en las traducciones.

También se puede encontrar una sección de preguntas frecuentes (FAQ) [6]. Como medios de soporte de la comunidad, se dispone de un foro [7].

COMUNIDAD

Número de usuarios

Es difícil hacer una estimación del número de descargas de clearOS, ya que la aplicación se descarga normalmente del apartado correspondiente en la web oficial [8] o desde los repositorios de las distribuciones. Aunque no se puede obtener un dato concreto, se puede deducir con esto que la distribución cuenta con una gran difusión entre los usuarios.

Foros y portales de ayuda

El usuario dispone de varias opciones para obtener ayuda: el foro y la sección de preguntas frecuentes (FAQ). Las FAQ no son un recurso de ayuda interactivo, pero se considera un portal de ayuda ya que es un buen recurso para resolver dudas.

Contribuciones

Se puede colaborar con el proyecto desarrollando aplicaciones y colaborando con las traducciones de la distribución y de su correspondiente documentación.

Frecuencia de versiones

La primera versión de clearOS de la que se conoce la fecha de publicación es la versión 5.1, a partir de ClarkConnect 5.0, publicada a principios de 2005. Desde entonces, se han ido liberando numerosas versiones con las correspondientes correcciones y mejoras, hasta llegar a la 6.2.0, versión estable actual de la distribución. Para más información sobre la trayectoria del proyecto, puede verse el timeline [9] disponible en su página web.

REFERENCIAS

[1] - http://www.clearfoundation.com/docs/howtos/manually_editing_firewall_rules

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

[3] - http://www.clearfoundation.com/docs/user_guide/5.0/system_requirements

[4] - http://www.clearfoundation.com/docs/user_guide/5.0

[5] - http://www.clearfoundation.com/docs/developer/start

[6] - http://www.clearfoundation.com/Frequently-Asked-Questions/clearfoundation-faq.html

[7] - http://www.clearfoundation.com/component/option,com_kunena/Itemid,232/

[8] - http://www.clearfoundation.com/Software/downloads.html

[9] - http://www.clearfoundation.com/Software/distribution-timeline.html