Análisis de aplicación: Cortafuegos de la distribución Zentyal

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 Zentyal
Versión: 2.2-2
Licencia: GPL
Idioma: Español
Web oficial: http://www.zentyal.com
Manual: http://doc.zentyal.org/es/firewall.html
Descripción básica: Zentyal es una distribución GNU/Linux para gestión de servidores, incluyendo la funcionalidad de cortafuegos entre varias otras, configurable mediante acceso por interfaz web. Fue diseñada para su uso en oficinas domésticas y PYMEs.

FUNCIONALIDAD

• División en cinco tipos de tráfico

De menos a más restrictivo, las clasificaciones del tráfico son:

- Tráfico de redes internas a Zentyal.

- Tráfico entre redes internas y de redes internas a Internet.

- Tráfico de Zentyal a redes externas.

- Tráfico de redes externas a Zentyal.

- Tráfico de redes externas a redes internas.

• Filtrado de paquetes o cortafuegos

El cortafuegos de Zentyal está **basado en IPTables**, de Netfilter. 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.

Las **políticas de acceso** de Zentyal están establecidas de forma que la configuración inicial sea lo más estricta posible, para garantizar la seguridad desde el primer momento. Así, tras la instalación, se establece que:

- El tráfico desde el exterior a Zentyal o a las redes internas no está permitido.

- El tráfico desde las redes internas a Zentyal está regulado a unos servicios específicos.

- El tráfico desde las redes internas o Zentyal al exterior está totalmente permitido.

Para la definición de **reglas de filtrado**, el administrador debe establecer cuatro elementos que definen cada una de estas reglas:

- Origen: cualquiera, una dirección IP o un objeto (dirección MAC o conjunto de IPs).

- Destino: cualquiera, una dirección IP o un objeto (dirección MAC o conjunto de IPs).

- Servicio: protocolos y puertos a los que se aplica la regla.

- Configuración de acceso: acción que se aplica a la conexión que cumple los requisitos.

Se dispone de tres **opciones de configuración de acceso**, seleccionables por el administrador para ser llevadas a cabo por las reglas definidas, aplicables a una conexión: permitir, denegar o registrar.

Las reglas de filtrado son evaluadas de arriba a abajo, y una vez que se acepta una conexión según una regla definida, no se evalúan más reglas. Por esto, puede que una regla genérica situada en la parte alta de la tabla de reglas anule una más específica situada en una posición más baja.

Puede encontrarse información más detallada acerca del cortafuegos de esta distribución en la documentación oficial de la comunidad Zentyal [2].

• **Redirección de puertos**

Es posible establecer un conjunto de **reglas de redirección de puertos** para las interfaces de red accesibles desde Zentyal. Al igual que para el filtrado, el administrador debe especificar el valor de una serie de elementos que definen la regla:

- Interfaz: interfaz donde se recibe el tráfico.
- Origen: cualquiera, una dirección IP o un objeto (dirección MAC o conjunto de IPs).
- Destino original: Zentyal, una dirección IP o un objeto.
- Puerto de destino original: cualquiera, un puerto determinado o un rango de puertos.
- Protocolo: protocolo al que se aplica la regla.
- Descripción: comentario sobre la regla (propósito, aclaraciones, etc.).

Opcionalmente, pueden registrarse las conexiones que cumplan la regla y sustituirse la dirección de origen para que se tome Zentyal como el origen de la conexión.

• **Otras funcionalidades de Zentyal**

- Servidor DNS: resolución de nombres de dominio.
- Servidor NTP: sincronización de hora.
- Servidor DHCP: configuración de red.
- Servidor HTTP: publicación de páginas web.
- Servidor FTP: transferencia de archivos.
- Autoridad de Certificación.
- Creación de VPNs.
- Sistema de Detección de Intrusos.
- ...

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

Siendo una interfaz sencilla en cuanto a diseño, los menús en algunos casos se encuentran muy escondidos, siendo necesario, en caso de no tener experiencia previa con Zentyal, tener que desplegar varios de ellos para encontrar la opción de configuración deseada.

La característica más destacable de la interfaz, en lo que a inconvenientes se refiere, es la necesidad de tener que guardar dos veces cada cambio que se efectúe sobre la configuración. Así, se requiere guardar los cambios pulsando en el botón incluido al final del formulario correspondiente y, después, confirmarlos en un botón ubicado en la esquina superior derecha de la interfaz web. Esto tiene un inconveniente añadido, y es que en pantallas con baja resolución o que no se adapten al formato de pantalla de Zentyal, este botón de confirmación de cambios puede no aparecer a la vista del usuario; también cabe destacar que, cuando los cambios no han sido todavía confirmados, este botón aparece en color rojo, en contraste con el color verde que presenta si no ha habido cambios todavía.

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 Zentyal. Su funcionalidad está basada en IPTables, incorporado en el framework Netfilter, disponible en todas las plataformas GNU/Linux.

Plugins

Zentyal permite ampliar su funcionalidad mediante la instalación de módulos adicionales, además de dar la posibilidad a los usuarios de desarrollar los suyos propios.

RENDIMIENTO

Requisitos hardware

Sistema operativo: Zentyal 2.2-2
Procesador: Desde P4 a Xeon Dual Core
Memoria RAM: Desde 1 hasta 8 GB
Espacio en disco: Desde 80 hasta 500 GB
Tarjeta Gráfica: No procede, se maneja por consola/interfaz web

Los requisitos hardware específicos dependerán del perfil de Zentyal que se requiera y la cantidad de usuarios que deba soportar el servidor. Puede encontrarse información detallada en el apartado de requisitos hardware de la web de Zentyal [3].

Consumo de memoria

La distribución Zentyal puede llegar a requerir de recursos de memoria ciertamente exigentes, 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.

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 la comunidad de Zentyal se puede encontrar una amplia documentación acerca del uso de las herramientas disponibles en la distribución. Esta información está totalmente disponible tanto en español como en inglés.

La página de documentación [4] que ofrece la comunidad del proyecto recoge gran variedad de documentos, incluyendo, además de los manuales de configuración pertinentes para cada uno de los perfiles disponibles, una guía de instalación, una guía de configuración inicial y un manual de actualización. Además, existe documentación para desarrolladores [5][6], donde se describen las formas de contribuir al proyecto desarrollando módulos adicionales.

También se puede encontrar una sección de preguntas frecuentes (FAQ) [7] y una wiki [8]. Como medios de soporte de la comunidad, se dispone de un foro [9] y un servicio de listas de correo [10].

COMUNIDAD

Número de usuarios

Es difícil hacer una estimación del número de descargas de Zentyal, ya que la aplicación se descarga normalmente del apartado correspondiente en la web oficial [11] 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: listas de correo, 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 módulos. Cualquier usuario puede unirse a las listas de correo, responder a preguntas de otros usuarios, documentar artículos, ejercer de tester y enviar informes y correcciones de errores.

Frecuencia de versiones

La primera versión de Zentyal de la que se conoce la fecha de publicación es la versión 1.2-1, publicada el 29 de Septiembre de 2009. Desde entonces, se han ido liberando numerosas versiones con las correspondientes correcciones y mejoras, hasta llegar a la 2.2-2, versión estable actual de la distribución. Actualmente está en fase beta la versión 2.3.

REFERENCIAS

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

[2] - http://doc.zentyal.org/es/firewall.html

[3] - http://doc.zentyal.org/es/installation.html#requisitos-de-hardware

[4] - http://doc.zentyal.org/es/

[5] - http://doc.zentyal.org/es/develop.html#entorno-de-desarrollo-de-nuevos-modulos

[6] - http://trac.zentyal.org/wiki/Documentation/Community/Document/Development/Tutorial

[7] - http://trac.zentyal.org/wiki/Documentation/Community/FAQ

[8] - http://trac.zentyal.org/wiki

[9] - http://forum.zentyal.org/

[10] - http://lists.zentyal.org/

[11] - http://www.zentyal.org/downloads/