Diseño e implementación de una topología segura

MariaJose.Santofimia@uclm.es
David.Villa@uclm.es

20 de noviembre de 2018

Las topologías de red seguras están diseñadas para facilitar la implementación de la política de seguridad de una infraestructura IT. En concreto, en este proyecto se va a utilizar la topología denominada *three legged firewall*, que se muestra en la siguiente figura.

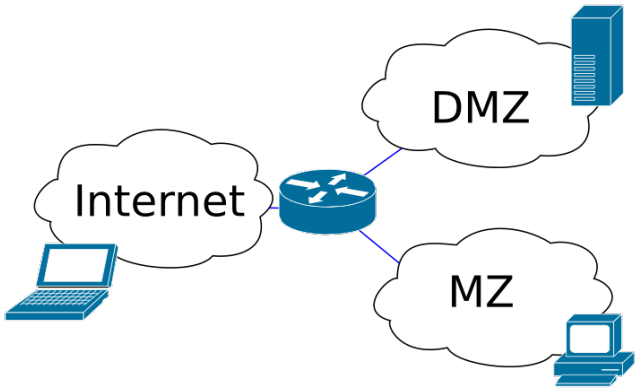

FIGURA 1: Topología de red segura

En este diagrama aparecen tres redes que tienen objetivos bien diferenciados:

- Red pública (Internet) sobre la que no tenemos ningún tipo de control.
- Red de servicios comunes (DMZ). Con acceso restringido para usuarios tanto externos (Internet) como internos (MZ).
- Red interna (MZ) a la que están conectados los empleados de la organización. Esta red no podrá ser accesible desde la red externa y de forma muy restringida desde la DMZ.

Dada una empresa dedicada a un propósito específico y elegida por el alumno (puede ser ficticia), el alumno debe implementar la topología de red explicada anteriormente. Por simplicidad se utilizarán máquinas virtuales VirtualBox para implementar los siguientes computadores:

- Encaminador perimetral: Alojará los servicios básicos DHCP, caché de DNS y las reglas de filtrado y encaminamiento.
- Servidor corporativo. En él habrán de instalar los servicios que la organización ofrece tanto a sus empleados como a los usuarios externos: servidor web, servidor de archivos, servidor de impresión, etc.
- Un PC estándar para emular el computador de un empleado. Aquí habremos de ejecutar al menos los clientes para comprobar que es posible acceder a los servicios especificados conforme a la política de seguridad.

Además, el computador del alumno (que ejecuta las máquinas virtuales) se utilizará también para emular un usuario externo que accede a los servicios de la DMZ en las condiciones indicadas en la política.

Características básicas de la red:

- La interfaz externa del encaminador obtendrá una dirección IP pública mediante un servidor DHCP que proporciona el ISP.
- Los servidores de la red DMZ tendrán direcciones IP estáticas.
- Los computadores de la red MZ obtendrán sus direcciones por medio de un servidor DHCP instalador en el encaminador.

Diseño de la política de seguridad

Sobre la base de la empresa elegida por el alumno, será necesario realizar un primer diseño de las cuestiones que serán abordadas por la política de seguridad. Para ello, considerará cuestiones como los distintos tipos de recursos que se deberán proteger (equipos de sobremesa, servidores, encaminador, aplicaciones, etc.), quienes tendrán acceso a los recursos y datos y en qué forma, lo críticos que son esos recursos o cómo protegerlos. La política de seguridad es un informe que define de forma clara y concisa los requisitos de seguridad, es decir, la privacidad e integridad de los servicios y datos.

Implantación de la política de seguridad

Una vez diseñada la política de seguridad, el siguiente paso será la implementación de la misma. En este sentido, se establecen una serie de requisitos mínimos en cuanto a las tecnologías a ser utilizadas:

- Monitorización y análisis de tráfico (Socket RAW).
- Filtrado de paquetes (`iptables`).
- NAT (`iptables`).
- DHCP (`dnsmasq`).
- DNS caché (`dnsmasq`).

Evaluación

Esta práctica se puntúa con un valor de 10 puntos sobre 25 de la actividad de laboratorio.

Los requisitos mínimos son:

- La red DMZ proporciona al menos un servicios (por ejemplo, web).
- Los usuarios de la MZ utilizan direccionamiento privado y pueden salir a Internet (NAT).

Para la obtención de la máxima nota se valora:

- La red DMZ proporciona varios servicios.
- Mejoras en las reglas de filtrado en base a las restricciones de la política de seguridad.
- Instalación de un servidor proxy.

- Registro de eventos en el firewall (por ejemplo, intentos de conexión prohibidos).
- Sistema que verifique que los registros son conforme a lo establecido en la política de seguridad.
- Generación de gráficos para ilustrar el contenido de los registros del firewall.

Condiciones y plazos

La práctica se podrá realizar en grupos de dos alumnos.

Como resultado, el grupo realizará una defensa oral y demostración de su trabajo en las últimas sesiones de laboratorio. También entregará en una tarea moodle un fichero ZIP o TGZ que incluya:

- Una breve memoria en formato PDF que describa los aspectos más imporantes del proyecto (dos páginas como máximo).
- Ficheros de configuración de todos los servicios involucrados.
- Scripts de captura y análisis.
- Otros ficheros creados o modificados por los alumnos.
- Un fichero de texto plano llamado README que indique la finalidad de cada uno de dichos ficheros y a qué servicio corresponden.