Protección de la interconexión de redes

Es muy raro que la red local de una empresa esté aislada. Su interconexión con Internet o cualquier otra red es algo normal. Por ello es necesario proteger las entradas y salidas de la red interna privada. Se pueden instalar diferentes equipos que se ocupen de esta protección.

1. Router de filtrado

Los mecanismos de filtrado que se pueden asociar a un router permiten el análisis de la capa 3 (de red) del modelo OSI.

El análisis de los paquetes entrantes y salientes se realiza, por ejemplo, en la cabecera IP, lo que permite acciones como:

- Bloqueo de direcciones IP (origen y destino).
- Prohibición de transmisión de protocolos de capa de Red o de Transporte utilizados (UDP, TCP o ICMP).

Algunos equipos incluyen las cabeceras de capa 4 (Transporte). Así pueden, entre otras cosas, realizar un filtrado en los puertos TCP o UDP e incluso realizar el análisis de datos de aplicación (capa 7).

2. Traductor de direcciones

En empresas grandes, distintas redes interconectadas pueden utilizar las mismas direcciones IP. Para que sea posible la comunicación entre nodos de los dos lados, hay que modificar las referencias del emisor del paquete, para que no haya conflicto y la transmisión sea fiable.

Los equipos de traducción de direcciones (NAT - *Network Address Translation*) se encargan de aportar esta funcionalidad. Permiten el cambio de una dirección IP por otra.

Hay tres tipos de traducción de dirección posibles:

- La traducción de puerto (PAT - *Port Address Translation*) funciona en una asignación dinámica de los puertos TCP o UDP, conservando la dirección IP original.
- La conversión dinámica de direcciones cambia la dirección IP instantáneamente, con relación a una externa disponible en una lista.
- La conversión estática de dirección, que también realiza un cambio de dirección IP, pero se mantiene una tabla que permite que se pueda sustituir una IP interna por la misma dirección IP externa.

Podemos observar que la conversión dinámica de direcciones permite disponer de menos direcciones externas que direcciones internas, lo que no ocurre en la conversión estática.

Una traducción de dirección IP también se puede realizar al salir de la red local. Esto permite ocultar la dirección privada interna. Este funcionamiento está previsto desde hace mucho tiempo y la RFC 1918 define rangos de direcciones utilizables en las redes privadas. Los tres espacios reservados son:

- 10.0.0.0, con una máscara de 8 bits (255.0.0.0).
- 172.16.0.0, con una máscara de 12 bits (de 172.16.255.254 a 172.31.255.254).
- 192.168.0.0, con una máscara de 16 bits (255.255.0.0).

Podemos observar que solo el primer rango de direcciones respeta el concepto de clase inicial, en este caso A.

Todas las demás direcciones son públicas y se pueden utilizar en Internet.

Así, por ejemplo, un equipo de la red local que realiza una solicitud a un sitio web en Internet verá su dirección IP de emisor traducida en una dirección pública al salir de la LAN.

3. Cortafuegos

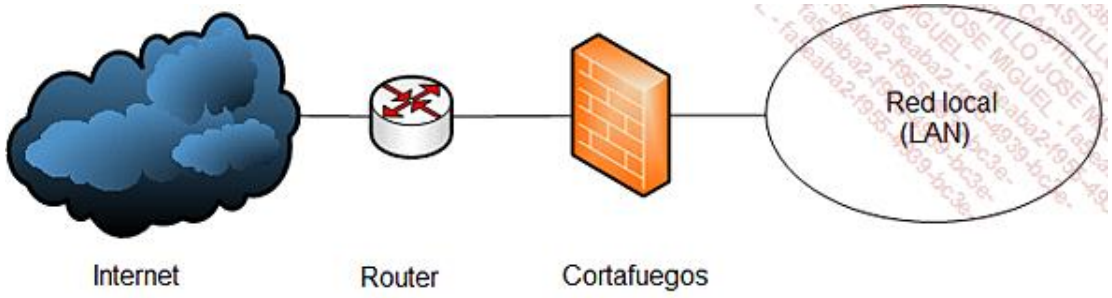
Un equipo de cortafuegos (*Firewall*) convierte las diferentes redes a las que se conecta en independientes. Al contrario que un router, no se conforma con transmitir la petición. Un cortafuegos segmenta los flujos asumiendo él mismo las peticiones. Para esto establece dos conexiones y puede realizar una acción de autenticación.

Esta segmentación también permite el cambio de la dirección del solicitante, como un mecanismo de traducción de direcciones.

La primera generación de estos equipos permitía distintos análisis en las cabeceras de los paquetes, de manera equivalente a los routers filtrantes. El cortafuegos de tabla de estado (*State full inspection*), más reciente, conserva en memoria una tabla de las conexiones establecidas. Así, las comunicaciones entre clientes, autorizadas después de la autenticación, pueden continuar sin problema.

La nueva generación de cortafuegos, llamada de aplicación, es capaz de analizar algunos cuerpos de paquetes, como los de los protocolos SMTP, HTTP... Este nivel de análisis permite atenuar las nuevas formas de ataque, que se aprovechan de los fallos de las aplicaciones estándar.

El cortafuegos de infraestructura suele ir acompañado de un cortafuegos personal, instalado en los equipos de trabajo. Así, los equipos se protegen de ataques que podrían proceder incluso de dentro de la red local.



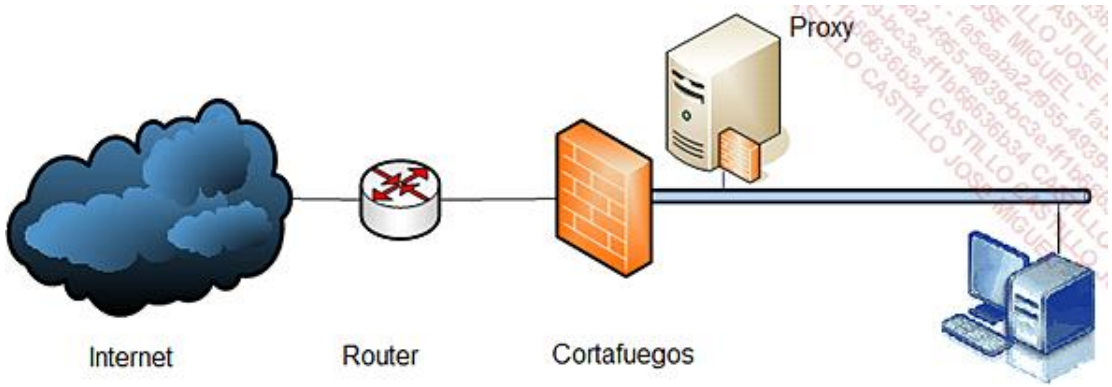
4. Proxy

El servidor proxy se utiliza especialmente en el ámbito del tráfico *Hyper Text Transfer Protocol* (HTTP), o incluso con *File Transfer Protocol* (FTP), en la red LAN e Internet. Se puede considerar que es un complemento del cortafuegos.

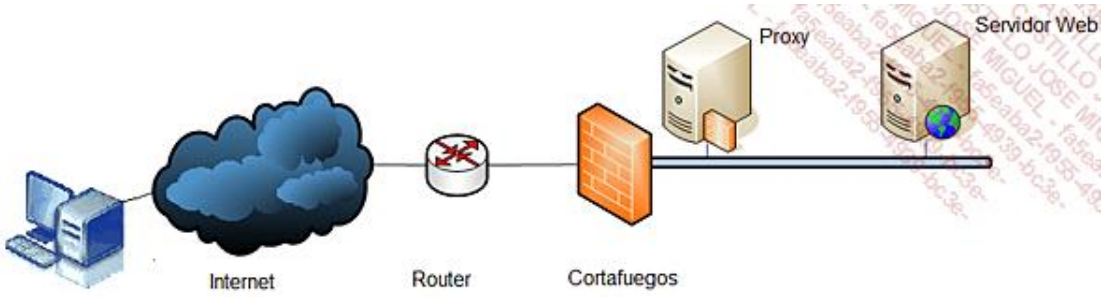
Cuando intercepta una petición hacia el exterior, el proxy la redirige como si fuera suya y a continuación almacena los datos recibidos. Seguidamente, los envía al solicitante inicial. Proxy es interesante por dos razones. En primer lugar, camufla las direcciones IP internas, puesto que la petición no llega a Internet. Y luego permite filtrar para, por ejemplo, prohibir el acceso a algunos sitios web.

Una tercera ventaja del proxy es su capacidad para administrar una memoria caché. Así pues, es posible volver a pedir un archivo o un sitio de Internet. A nivel web, esta función es relativa. De hecho, un sitio dinámico cambia tan

a menudo que se puede considerar que se carga en cada petición.



Un servidor proxy inverso (*reverse proxy*) intercepta una petición, por ejemplo de un sitio web, procedente del exterior hacia un servidor interno. Esto permite evitar que estas peticiones lleguen a un servidor más vulnerable.

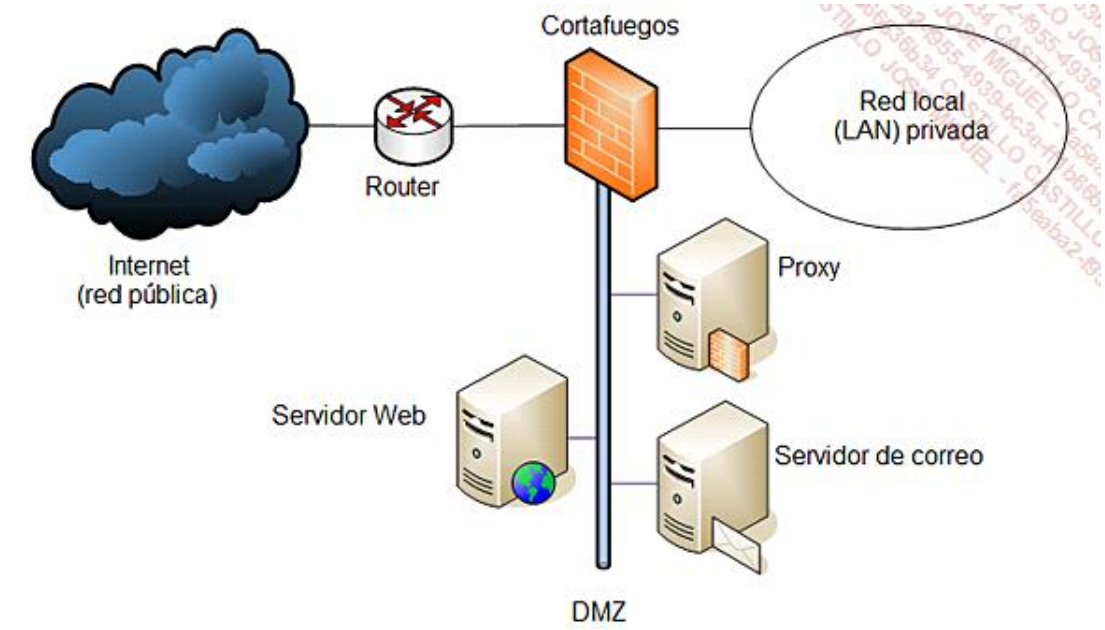


5. Zona desmilitarizada

La interconexión entre la red pública Internet y la LAN a menudo utiliza una zona pública de *buffer* que está en la propia empresa. Esta zona se denomina «zona desmilitarizada» o *DeMilitarized Zone* (DMZ). Puede albergar diferentes servidores accesibles desde Internet, como:

- El servidor Proxy.
- El servidor web que alberga el sitio de la empresa.
- El servidor de correo, encargado de seleccionar los mensajes.

La frontera de esta DMZ se concreta con al menos un cortafuegos. En infraestructuras de pequeño tamaño, suele ser un servidor para todo. En este caso, se le denomina trirresidente.



Las infraestructuras de mayor envergadura albergan una DMZ protegida por dos cortafuegos, uno por delante y otro por detrás. En este caso, se configuran de manera complementaria y generalmente son de marcas diferentes para que no presenten las mismas vulnerabilidades.