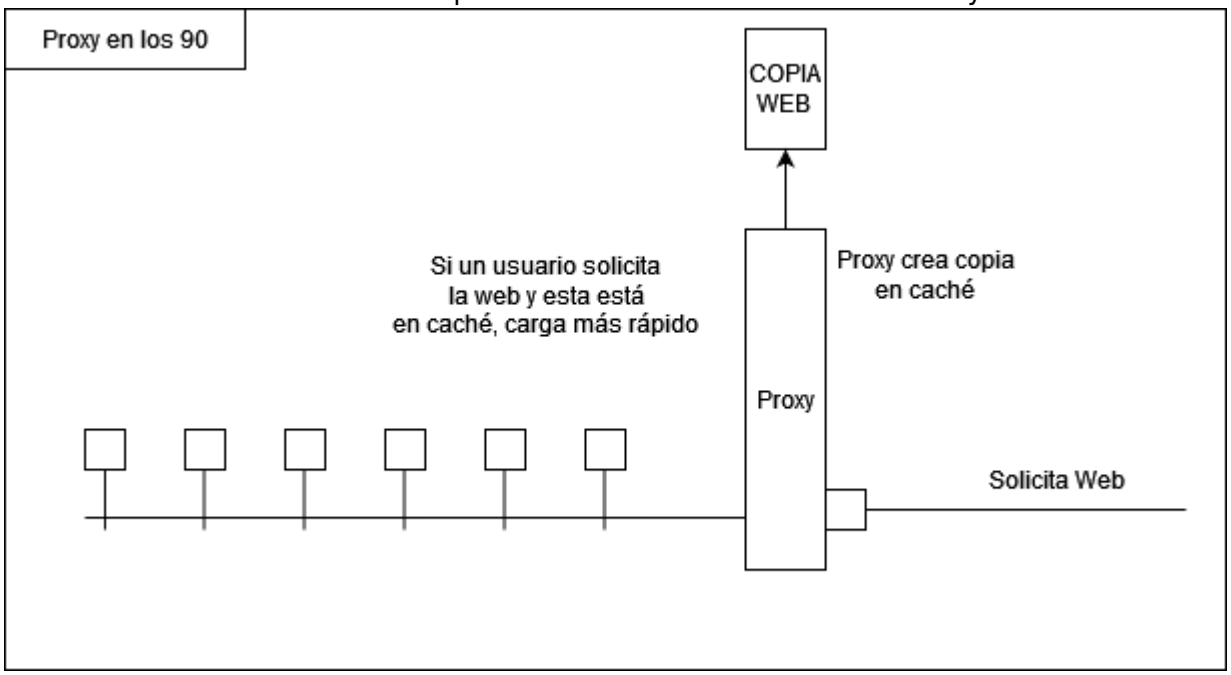
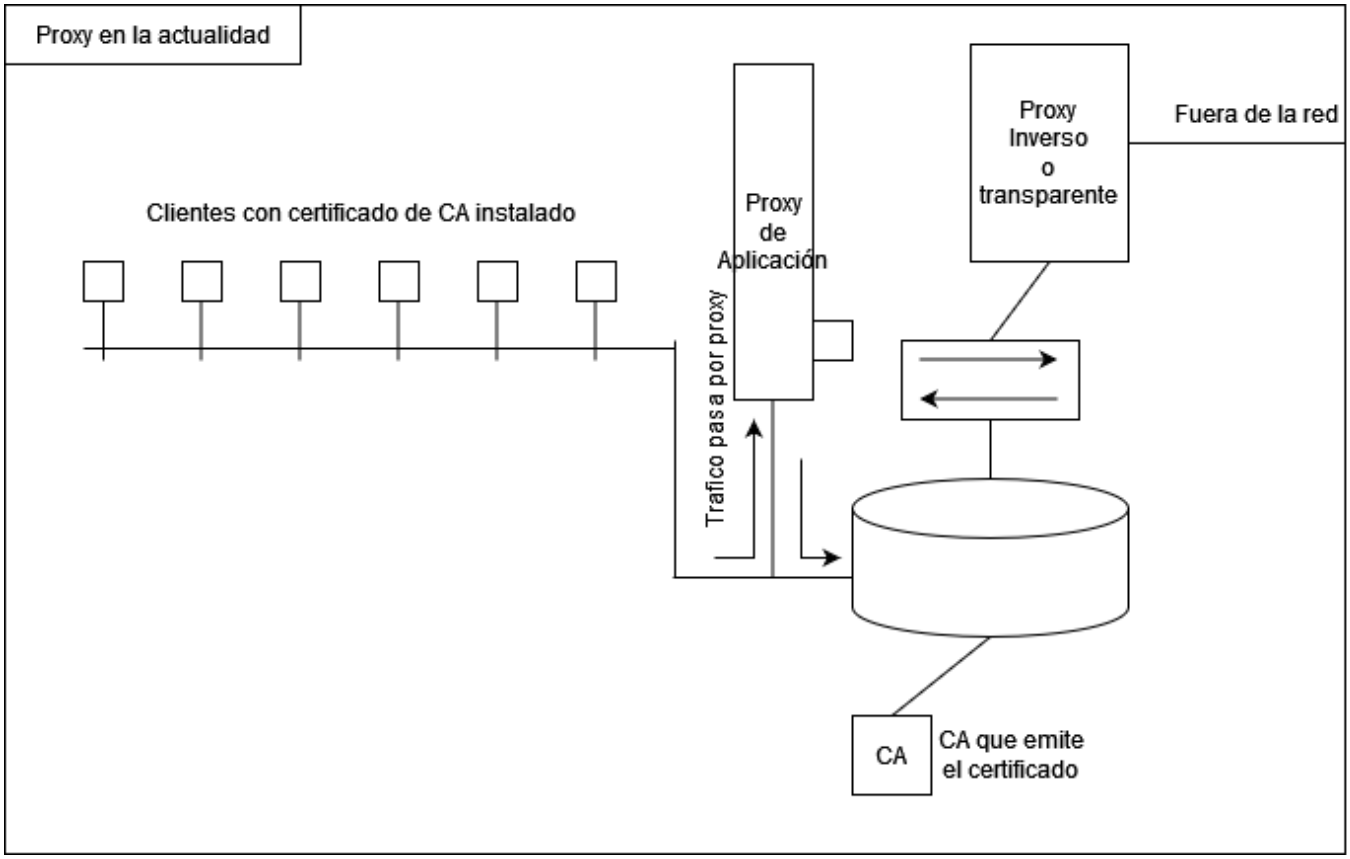
Servidores Proxy

Vamos a ver un elemento de seguridad adicional para complementar con los elementos que ya se encuentran en una red corporativa. Es un dispositivo software que actía como intermediario entre un cliente y un servidor. Es un dispositivo que intercepta las conexiones. La principal diferencia entre router y proyx es firewall enruta y el proxy no, el proxy captura una conexión y establece una nueva. Los proxy de base eran dispositivos para la aceleración de ancho de banda en los años 90, lo que hacían era almacenar contenidos para aumentar la velocidad de acceso y ahorrar ancho de banda.



Si un proxy guarda logs SIEMPRE deben ser dados de alta en la Agencia de Protección de Datos. En la actualidad ya no se usan para aumentar la velocidad. Se usan para controlar posible malware, aplicar políticas de acceso a internet o para exfiltración de información.



Con una topología como esta se puede hacer que todo el tráfico de red salga por el proxy con una ACL. El proxy puede comprobar si hay algún tipo de malware o si el trafico que pasa por el está permitido y en función de que sea bloquearlo o dejarlo pasar. Hay varios tipos de proxy:

- Capa de aplicación: Web Proxy o email proxym existen dos conexiones, una entre el PC y el proxy y otra entre el proxy y el servidor externo. Para que sean efectivos estos proxy tienen que manejar e implementar los protocolos de capa de aplicación: Web Security Appliance, Email Security Appliance. Facilitan el proceso de autenticación (cuando sea necesaria).
- Proxy Inverso: Revisa que no se estén intentado realizar ataques de inyección SQL o XSS, añadiendo protección extra a equipos que dan servicios fuera de la red.
- Proxy transparente: Proxy que no ve el usuario. Para solucionar problemas con el tráfico cifrado se despliega una PKI para proporcionar certificados firmados a los clientes. Un problema de estos proxy es que soporta un número limitado de protocolos

Directrices

Los proxy pueden ir detras del firewall de filtrado de paquetes o puede estar en una red externa. Los servicios que se suelen proxymizar son Web y Correo Electrónico ya que son los principales vectores de entrada de malware en la actualidad.

Soluciones

- Squid
- HA Proxy
- Nginx
- Sophos

- Zscaker