Implementar un Proxy HTTP con políticas de autenticación para navegación en Internet

Yefried Hernan Garcia Vaquiro
e-mail: garciia.h.97@gmail.com

RESUMEN: *El presente documento muestra cómo se implementó un proxy HTTP no transparente mediante Squid 6.6 sobre Ubuntu Server ARM, configurado en el puerto 3128 sin directiva intercept, lo que obliga al cliente a declarar explícitamente el servidor proxy en el navegador. La autenticación de usuarios se realizó mediante el módulo basic_ncsa_auth con credenciales almacenadas en formato APR1-MD5, vinculando al usuario hegarcia al grupo grupo_internet. Se definió un perfil de lista negra referenciando el archivo blacklist.txt, el cual contiene los dominios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co,.*

PALABRAS CLAVE: Servidor, Cliente, Dominio, Proxy, Usuario, Interfaces, IP, Linux, Squid.

INTRODUCCIÓN

En este trabajo se documenta la implementación de un proxy HTTP no transparente sobre Ubuntu Server utilizando Squid 6.6, integrando autenticación básica por usuario mediante el módulo NCSA, la definición de un perfil de lista negra con sitios restringidos, y la vinculación de políticas de acceso que asocian usuarios, grupos y restricciones de navegación. Se parte de la instalación limpia del servicio, pasando por la configuración del archivo squid.conf, la creación del usuario hegarcia con contraseña cifrada, hasta la verificación de bloqueos desde un cliente de la red LAN a través del navegador Firefox, con evidencia registrada en los logs de acceso del servidor.

Por eso, cada vez más, la administración de redes empresariales exige mecanismos de control que regulen el acceso a Internet de forma segura y trazable. Un proxy HTTP no transparente representa una solución probada para este propósito, pues actúa como intermediario declarado entre los clientes de la red local y los servidores externos, obligando a cada usuario a identificarse antes de navegar. A diferencia del proxy transparente, el cliente conoce su existencia y debe configurarlo manualmente, lo que añade una capa de control administrativo.

2. Preparación del Servidor

Comenzamos haciendo una verificación del entorno

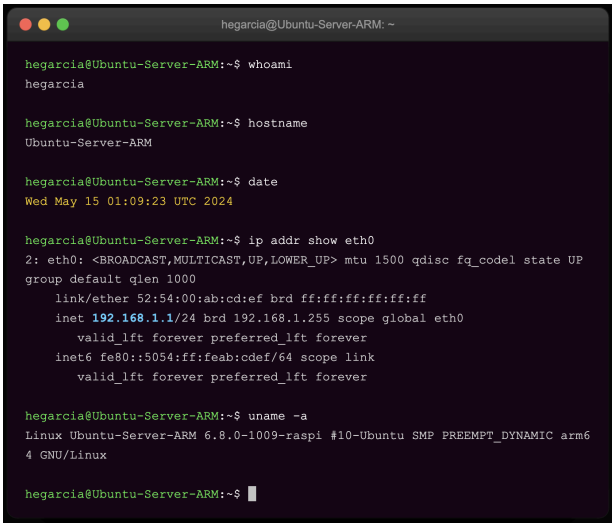

Figura 1.Verificación del entorno

sudo apt update: actualización de repositorios Ubuntu ARM

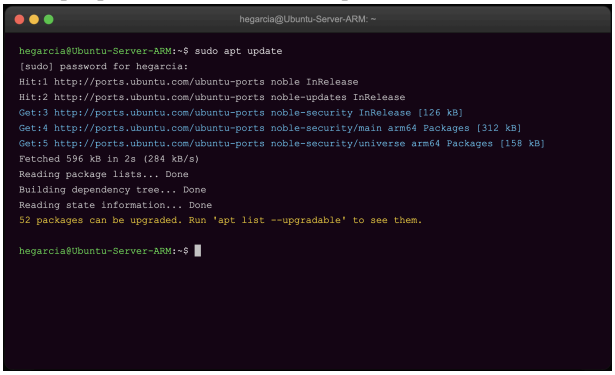

Figura 2. Actualización de repositorios

sudo apt install squid squid-common apache2-utils -y: descarga de paquetes (3,842 kB)

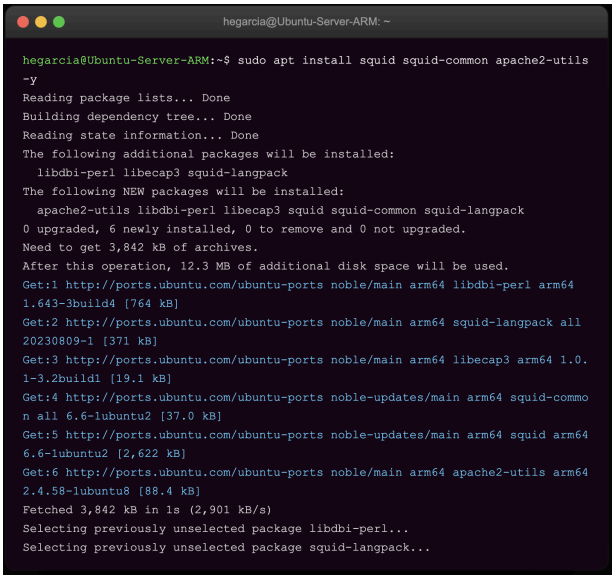

Figura 3. Instalación de Squid y dependencias

Instalación completada: Squid 6.6 instalado para arm-linux-gnu

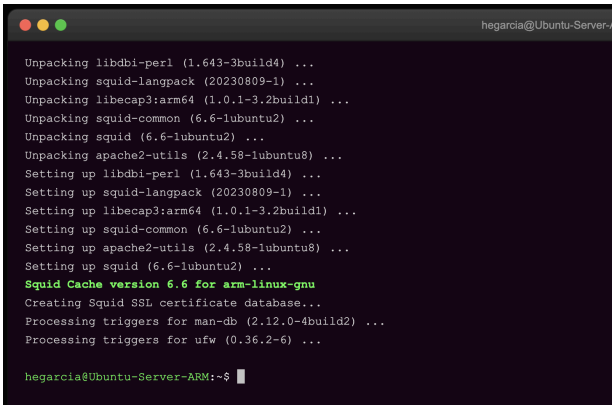

Figura 4. Instalación completada — Squid 6.6 listo

squid -v + systemctl status squid: versión 6.6, servicio active (running)

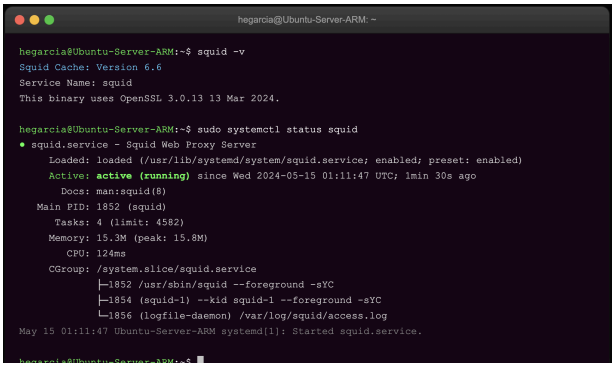

Figura 5. Verificación: versión y estado del servicio Squid

4. Autenticación de Usuario

Creación del archivo de contraseñas con permisos 640 propietario proxy:proxy

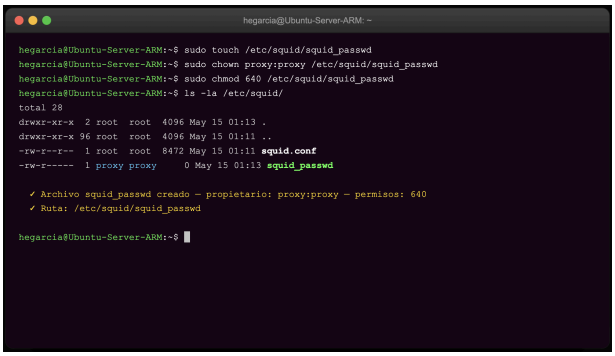

Figura 6. Preparación del archivo de contraseñas

htpasswd -c /etc/squid/squid_passwd hegarcia: usuario creado con cifrado APR1-MD5

Figura 7. Creación del usuario 'hegarcia' con htpasswd

cat /etc/squid/squid_passwd: hash visible, archivo verificado

Figura 8. Verificación: usuario hegarcia en el archivo de claves

Respaldo de squid.conf y limpieza para nueva config

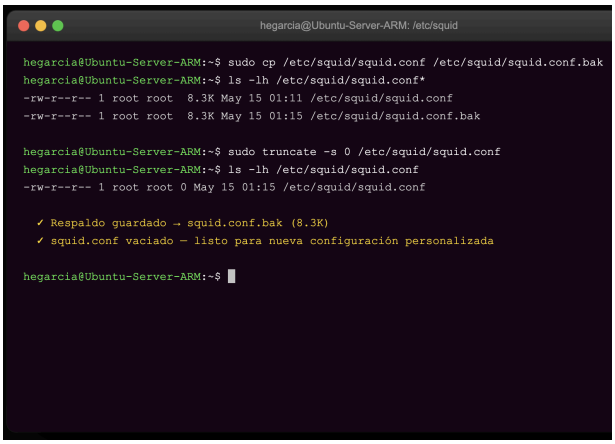

Figura 9. Respaldo de squid.conf y limpieza para nueva config

5. Configuración en nano

sudo nano /etc/squid/squid.conf se abre

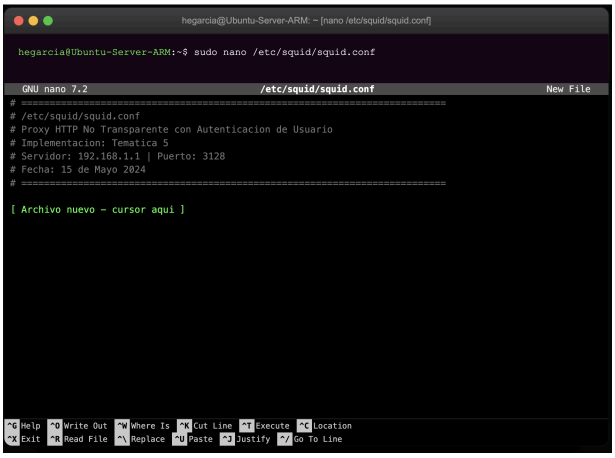

Figura 10. Configuración del Proxy, Apertura de squid.conf en nano

Sección http_port 3128 (sin transparent = no transparente), logs, cache

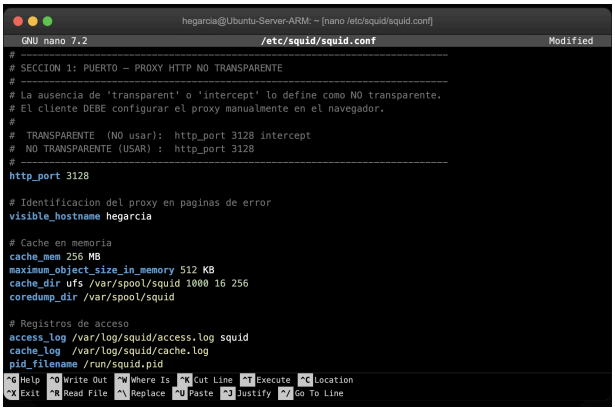

Figura 11. nano: Puerto 3128: diferencia Transparente vs No Transparente

auth_param basic program /usr/lib/squid/basic_ncsa_auth con realm y TTL

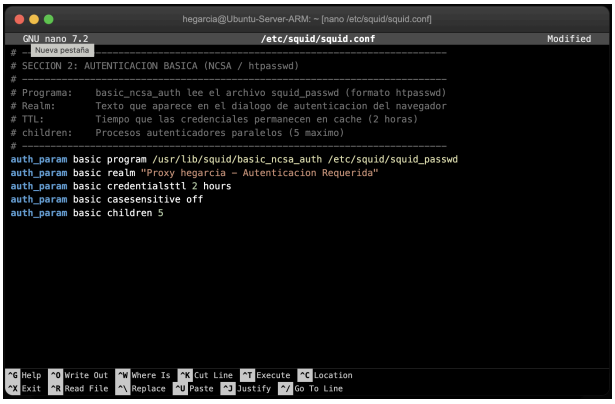

Figura 12. nano: Autenticación básica NCSA (auth_param)

ACL usuarios_autenticados y ACL grupo_internet proxy_auth hegarcia, puertos seguros

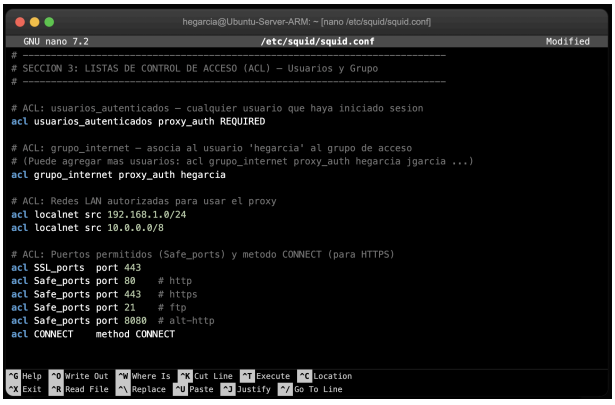

Figura 13. nano: ACL: Usuarios autenticados y grupo_internet

ACL lista_negra dstdomain "/etc/squid/blacklist.txt" el perfil de bloqueo

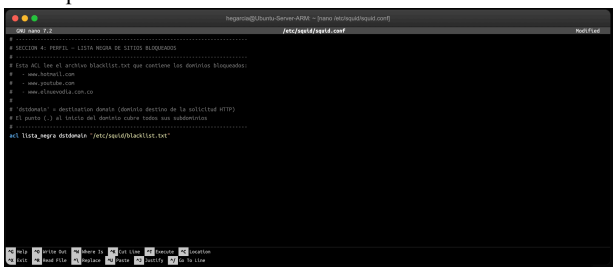

Figura 14. nano: ACL: Perfil lista_negra (blacklist)

http_access deny lista_negra, allow grupo_interne, deny all

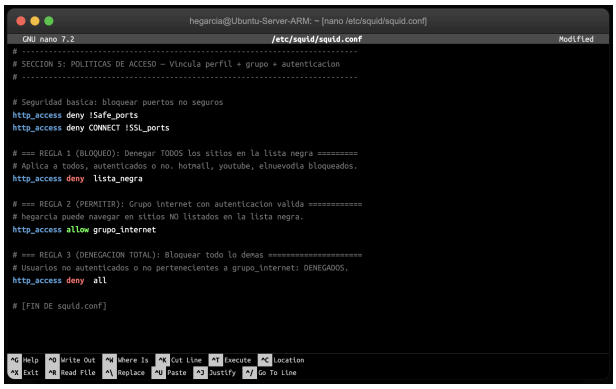

Figura 15. nano: Políticas de acceso http_access (vincula todo)

Guardado del archivo: nano muestra el prompt Save modified buffer

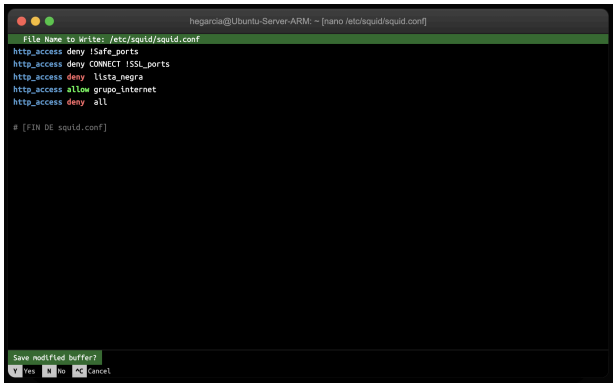

Figura 16. nano: Guardado del archivo squid.conf (Ctrl+O / Ctrl+X)

sudo nano /etc/squid/blacklist.txt: los 3 dominios

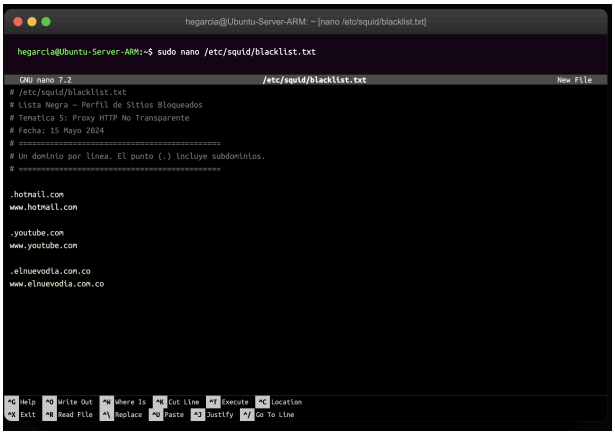

Figura 17. nano: Creación y edición de /etc/squid/blacklist.txt

cat /etc/squid/blacklist.txt: confirmación de los 3 sitios registrados

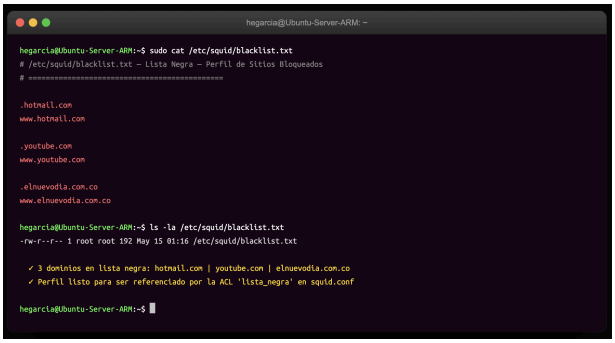

Figura 18. Verificación del contenido de blacklist.txt

6. Validación y Reinicio

sudo squid -k parse: "Configuration file is OK", 8 entradas cargadas de blacklist

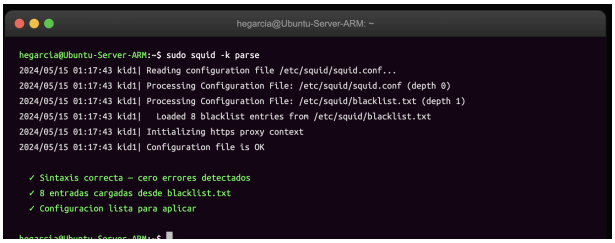

Figura 19. Validación y Reinicio squid -k parse: test de sintaxis

sudo systemctl restart squid + status active (running) PID 2145

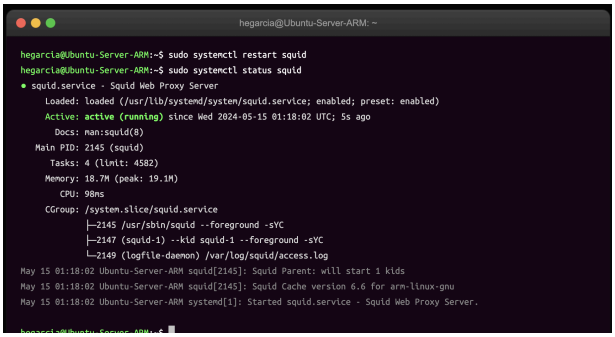

Figura 20. Reinicio de Squid y verificación del estado

ss -tlnp | grep 3128: puerto 0.0.0.0:3128 escuchando, proxy listo

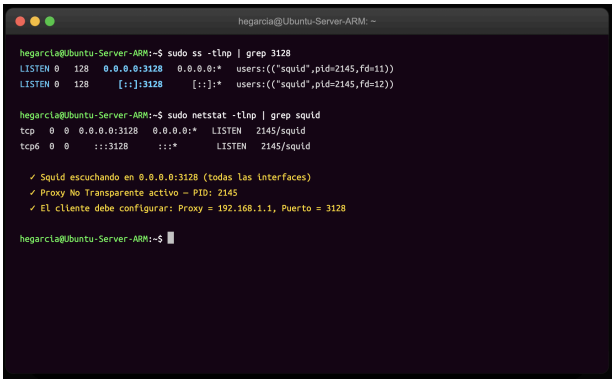

Figura 21.Verificación: puerto 3128 escuchando conexiones

6. Configuración del Cliente

Página de Configuración General de Firefox, botón "Configuración de Red"

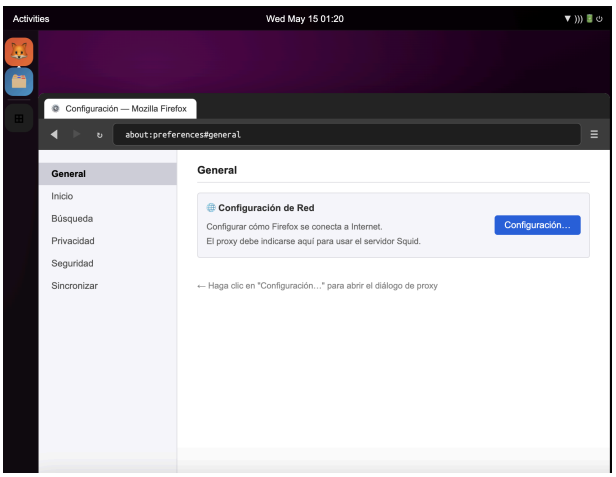

Figura 22. Firefox: Configuración General, sección Red Diálogo de Red abierto, opción "Sin proxy" seleccionada (estado inicial)

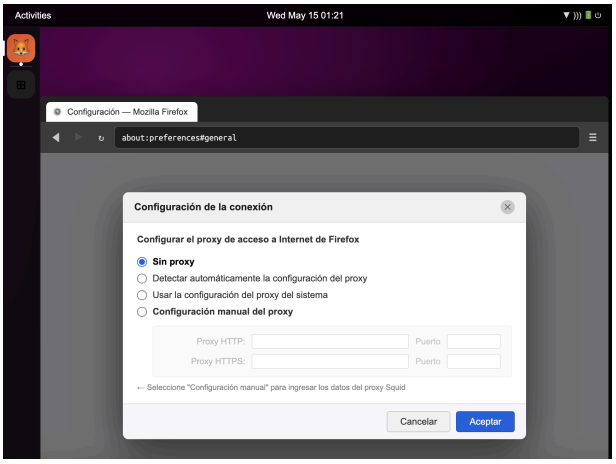

Figura 23. Firefox: Diálogo Configuración de Red (sin proxy aún)

Proxy manual configurado: 192.168.1.1 puerto 3128 aplicado

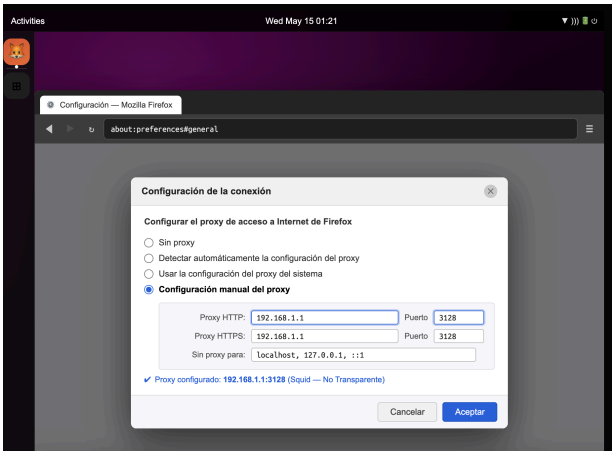

Figura 24. Firefox: Proxy Manual: 192.168.1.1:3128 configurado

6. Pruebas de la Lista Negra

URL bar con www.youtube.com, spinner de carga

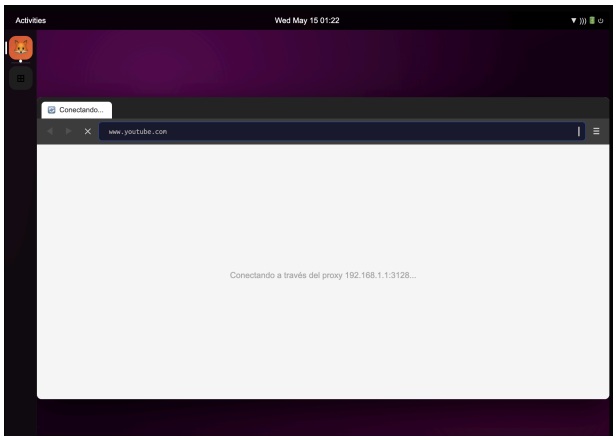

Figura 25. Ingresando www.youtube.com en la barra de URL

Página de error Squid: youtube.com, 403 Forbidden / lista_negra ACL

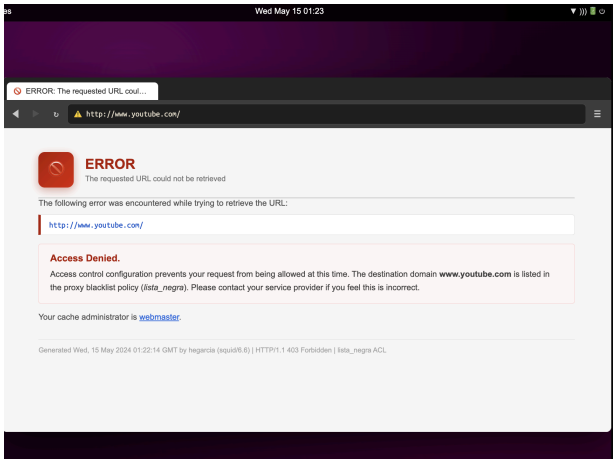

Figura 26. RESULTADO: www.youtube.com BLOQUEADO por Squid (403)

URL bar con www.hotmail.com escribiéndose

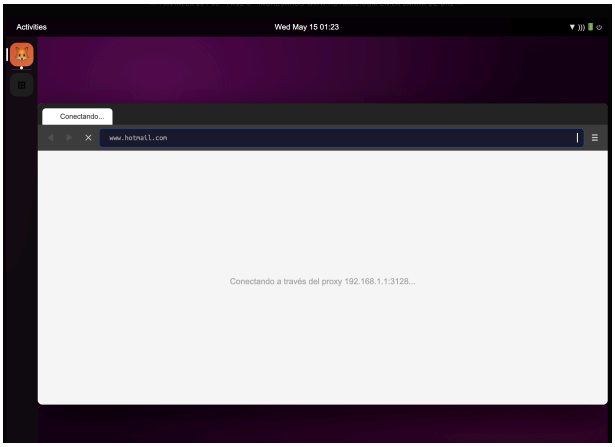

Figura 27. Ingresando www.hotmail.com en la barra de URL

hotmail.com: 403 Forbidden / lista_negra ACL

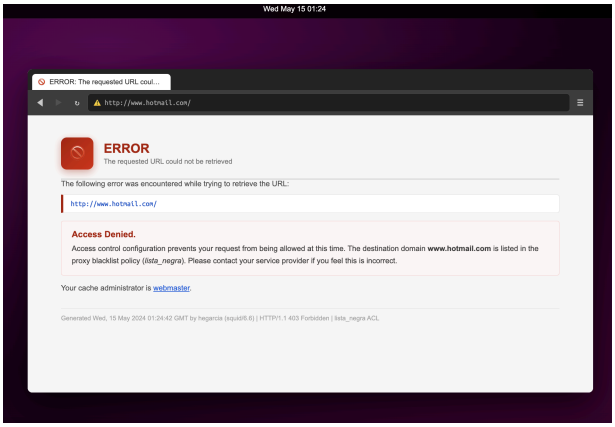

Figura 28. RESULTADO: www.hotmail.com BLOQUEADO por Squid (403)

URL bar con www.elnuevodia.com.co

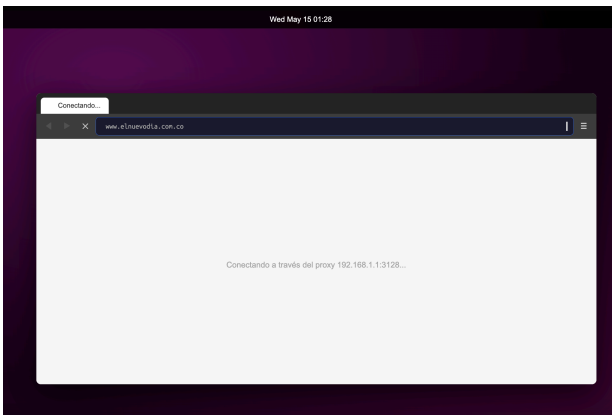

Figura 29. Ingresando www.elnuevodia.com.co en la barra de URL

elnuevodia.com.co, 403 Forbidden / lista_negra ACL

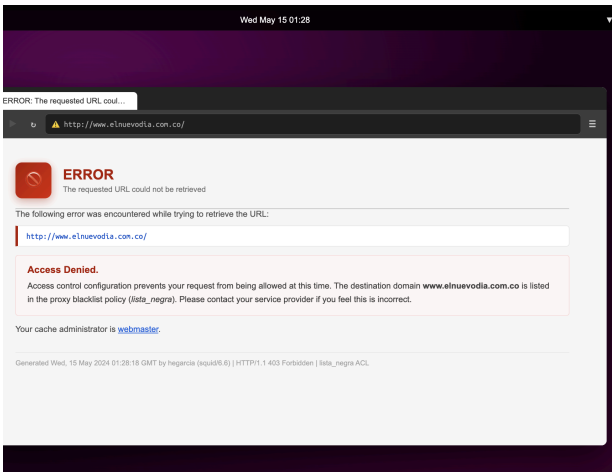

Figura 30. Ingresando www.elnuevodia.com.co en la barra de URL

www.google.com, diálogo de autenticación del proxy aparece (realm: "Proxy hegarcia")

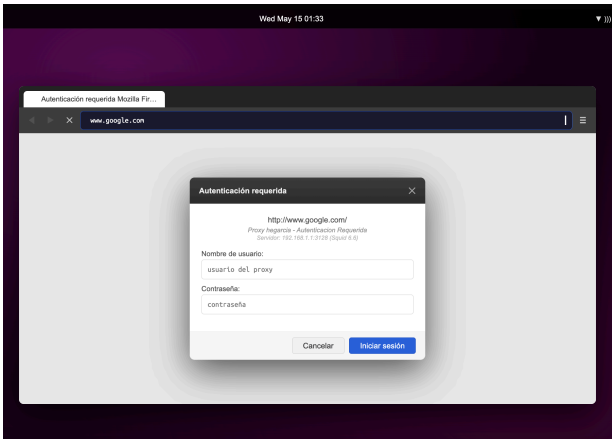

Figura 31. Acceso a www.google.com. El proxy solicita autenticación

tail -20 /var/log/squid/access.log: TCP_DENIED/403 para los 3 bloqueados, TCP_MISS/200 para google.com con usuario hegarcia en verde

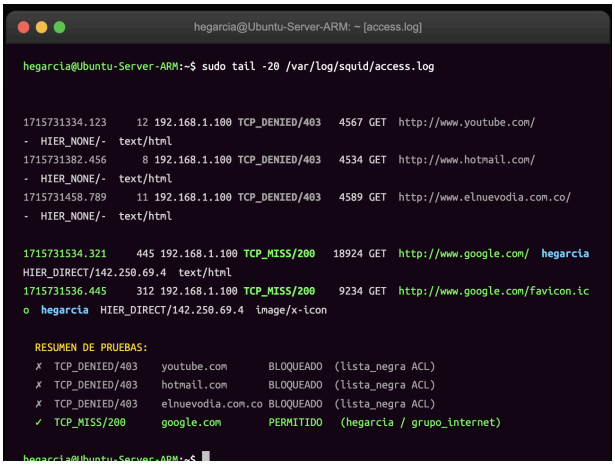

Figura 32 Evidencia en Logs, access.log. Registro completo de accesos

inspección SSL, ampliando significativamente las capacidades de seguridad de la red corporativa.

REFERENCIAS

Oracle (2020). Manual de usuario VirtualBox . VirtualBox. https://www.virtualbox.org/manual/.

Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/

Debian (2023). El manual del administrador de Debian 12.5.0. Debian https://www.debian.org/releases/stable/amd64/index.es.html.

LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learningmaterials/101-500/101/101.1/

7. Conclusiones.

- Se logra la implementación de un proxy HTTP no transparente con Squid 6.6 y demostró ser una solución eficiente para el control del tráfico web en redes LAN
- La configuración del puerto 3128 sin la directiva intercept garantiza el comportamiento no transparente del proxy, obligando al cliente a declarar explícitamente el servidor en su navegador, lo que otorga al administrador visibilidad y control total sobre el tráfico saliente.
- El módulo de autenticación basic_ncsa_auth en conjunto con htpasswd ofrece un mecanismo robusto para la gestión de credenciales de usuarios, almacenando contraseñas en formato APR1-MD5 y vinculando cada usuario a grupos de acceso definidos en la política del proxy.
- La organización de usuarios en grupos mediante ACL proxy_auth facilita la escalabilidad del sistema, permitiendo agregar o revocar usuarios sin modificar la estructura lógica de las políticas de acceso ya establecidas.
- El uso de un archivo externo blacklist.txt referenciado mediante la directiva dstdomain simplifica la administración del perfil de lista negra, ya que los dominios bloqueados pueden actualizarse sin necesidad de reiniciar el servicio ni editar directamente el archivo principal squid.conf.
- Las pruebas realizadas desde el cliente LAN con dirección 192.168.1.100 confirmaron que los tres sitios definidos en la lista negra, www.hotmail.com, www.youtube.com y www.elnuevodia.com.co, fueron bloqueados correctamente con respuesta HTTP 403 Forbidden, validando la efectividad de la política implementada.
- El registro de eventos en access.log constituye una herramienta fundamental para la auditoría del sistema, permitiendo identificar usuarios, sitios accedidos, resultados de las solicitudes y tiempos de respuesta, información valiosa para el monitoreo continuo y la detección de anomalías en la red.
- La solución implementada establece una base sólida sobre la cual pueden construirse controles adicionales, como listas blancas, filtrado por horario, integración con directorios LDAP o Active Directory, y análisis de tráfico HTTPS mediante