Implementación de Proxy HTTP No Transparente con Políticas de Autenticación para Navegación Segura en Internet

Suescun, Jose Daniel

Universidad Nacional Abierta y a Distancia (UNAD)

jdsuescunc@unadvirtual.edu.co

***Abstract*— *Este documento presenta la implementación y configuración de un servidor proxy HTTP no transparente utilizando Endian Firewall, una solución integral de seguridad de código abierto basada en GNU/Linux. El objetivo es establecer políticas de autenticación y mecanismos de control de acceso para la navegación en Internet dentro de entornos corporativos. La implementación demuestra cómo el software libre puede proporcionar características de seguridad de nivel empresarial para la gestión del tráfico de red.*

I. INTRODUCCIÓN

En los entornos organizacionales contemporáneos, la gestión y seguridad del tráfico de red representa un desafío crítico para los administradores de infraestructura TI. El crecimiento exponencial de servicios basados en Internet ha necesitado la implementación de mecanismos de seguridad robustos que puedan controlar y monitorear efectivamente el acceso de usuarios a recursos externos mientras se protegen los datos internos sensibles.

Los servidores proxy han emergido como componentes esenciales en las arquitecturas de seguridad de red, sirviendo como intermediarios entre los clientes de la red interna y los recursos externos de Internet. Los proxies HTTP configurados con políticas de autenticación proporcionan a las organizaciones un control granular sobre el acceso web, permitiendo hacer cumplir políticas de seguridad y optimizar la utilización del ancho de banda.

II. DESARROLLO DE CONTENIDOS

A. Fundamentos Teóricos

1) Servidores Proxy: Los servidores proxy funcionan como sistemas intermediarios que procesan solicitudes de clientes y las reenvían a servidores de destino. En contextos de seguridad de red, los proxies proporcionan filtrado de contenido, capacidades de caché y control de acceso centralizado.

2) Endian Firewall: Es una solución UTM (Unified Threat Management) de código abierto construida sobre GNU/Linux. Integra Squid proxy para gestión de tráfico HTTP/HTTPS, iptables para firewall, y servicios de seguridad adicionales.

B. Diseño de Infraestructura

La implementación utilizó un entorno virtualizado con tres componentes: Zona Verde (LAN Interna) con estaciones Debian, Zona Roja (WAN Externa) con conexión simulada a Internet, y Zona Naranja (DMZ) con Ubuntu Server. Endian Firewall gestiona el flujo de tráfico entre zonas implementando políticas de seguridad.

III. IMPLEMENTACIÓN

A. Instalación de Endian Firewall

Endian Firewall Community Edition 3.3.2 fue desplegado en máquina virtual. La configuración inicial involucró selección de idioma, configuración de modo de red, asignación de interfaces a zonas de seguridad y configuración de direcciones IP por zona. El proceso completó exitosamente, proporcionando acceso a la interfaz administrativa web.

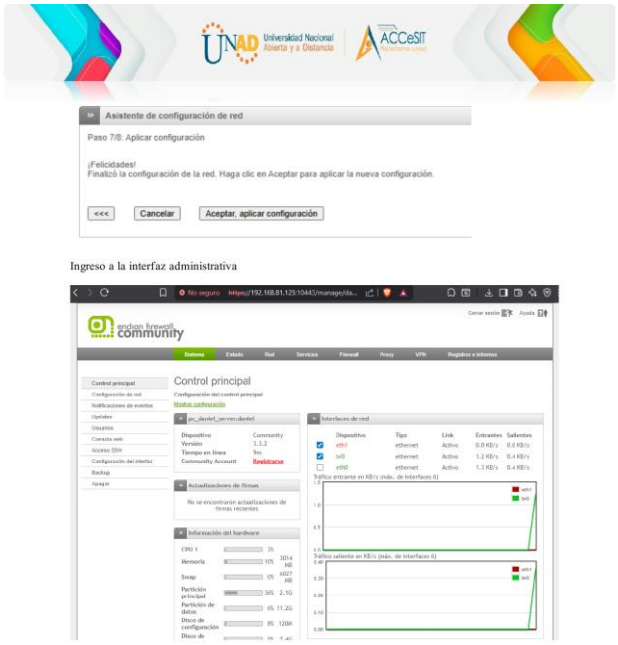

Figura 1

Panel Principal de Endian Firewall Mostrando el Estado del Sistema

Figura 2

Configuración de Autenticación del Proxy HTTP con Creación de Usuario

B. Configuración NAT

Se establecieron reglas de Traducción de Direcciones de Red para habilitar conectividad saliente. NAT de Origen (SNAT) fue configurado para traducir direcciones privadas a interfaz externa. NAT de Destino (DNAT) permitió acceso externo selectivo a servicios DMZ mediante reenvío de puertos HTTP y FTP.

C. Implementación del Proxy HTTP

1) Autenticación de Usuarios: Se creó usuario 'daniel' asociado al grupo 'bloqueo-redes'. El proxy fue configurado para requerir credenciales antes de procesar solicitudes, integrándose con el sistema de autenticación de Endian. La Figura 2 muestra la configuración de autenticación y la creación del grupo de usuarios.

2) Perfil de Filtrado: Se creó perfil 'bloqueo' con lista negra de dominios prohibidos: www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. El filtrado opera en capa de aplicación examinando encabezados HTTP. La Figura 3 ilustra la configuración del grupo y la lista negra de sitios web bloqueados.

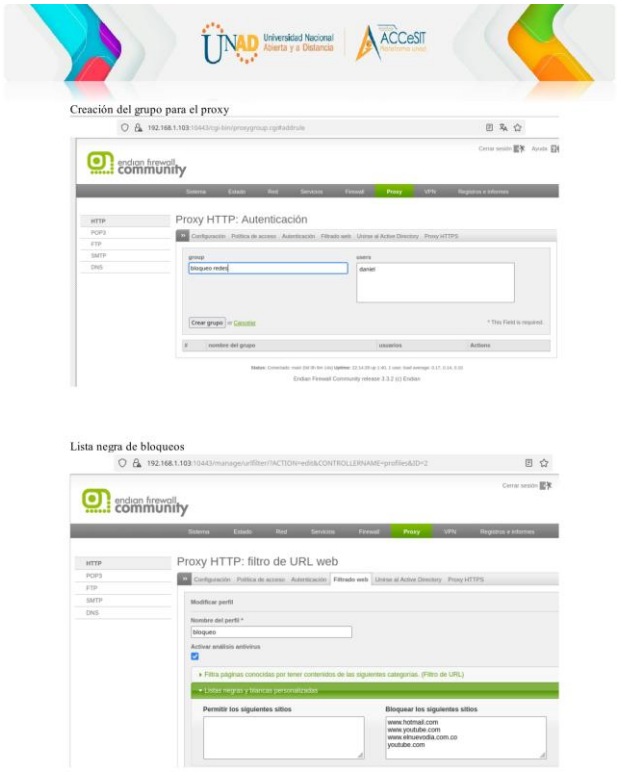

Figura 3

Creación del Grupo Bloqueo-Redes y Configuración de Lista Negra

3) Política de Acceso: Configurada vinculando grupo de usuarios, sin restricciones de tiempo, todos los navegadores permitidos, y perfil de filtrado aplicado con prioridad máxima en evaluación. La Figura 4 presenta la configuración completa de la política de acceso del proxy.

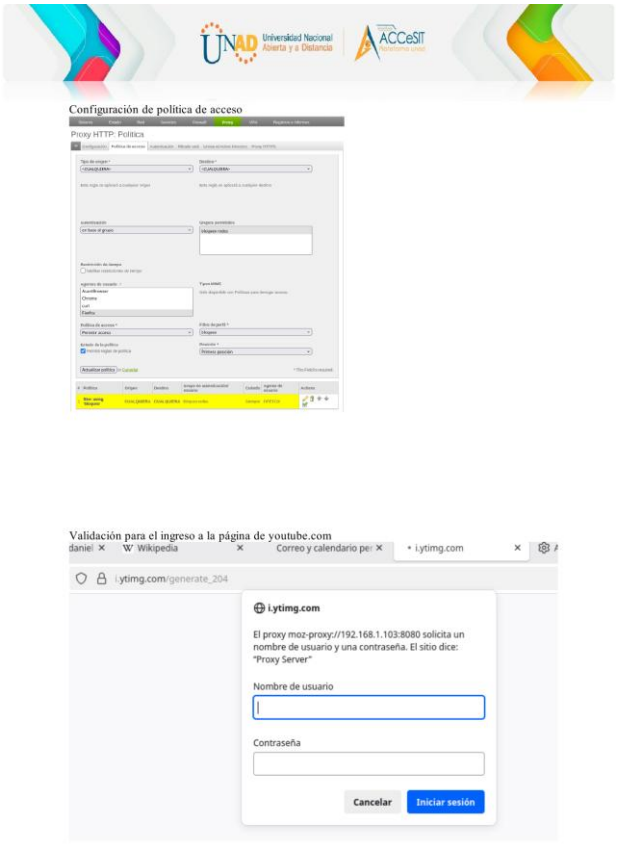

Figura 4

Configuración de Política de Acceso del Proxy HTTP

IV. RESULTADOS Y ANÁLISIS

A. Validación de Autenticación

Navegadores configurados para proxy en puerto 8080 presentaron exitosamente desafíos de autenticación. El mecanismo validó correctamente credenciales y otorgó acceso según políticas, demostrando integración efectiva entre gestión de usuarios y framework de autenticación Squid.

B. Efectividad del Filtrado

Los intentos de acceso a dominios en lista negra resultaron en denegación apropiada. Pruebas confirmaron bloqueo exitoso generando mensajes 'Access Denied'. El proxy identificó correctamente nombres de dominio antes de establecer conexiones, operando en capa de aplicación mediante búsquedas

hash eficientes. La Figura 5 muestra el bloqueo efectivo del sitio hotmail.com.

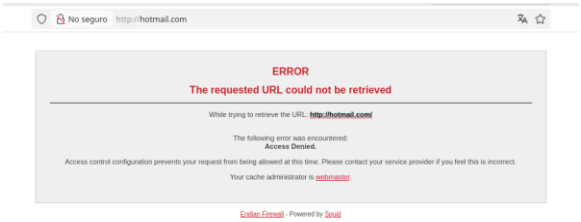

Figura 5

Bloqueo Efectivo del Sitio Web Hotmail.com por el Proxy HTTP

C. Segmentación de Red

La arquitectura DMZ aisló exitosamente servicios web de red interna permitiendo acceso controlado. Clientes internos accedieron servicios DMZ mediante reglas explícitas, mientras se previno acceso directo desde redes externas. La configuración NAT ocultó esquemas de direccionamiento internos.

V. DISCUSIÓN

La implementación demuestra ventajas de soluciones de seguridad de código abierto. Endian Firewall proporciona capacidades de nivel empresarial sin costos de licenciamiento, haciendo características avanzadas accesibles a organizaciones con presupuestos limitados. La base GNU/Linux permite personalización profunda mientras la interfaz web simplifica tareas administrativas.

La madurez de Squid y el soporte comunitario aseguran confiabilidad. La combinación de componentes crea una plataforma integral que requeriría múltiples productos propietarios para replicar, reduciendo costos y complejidad.

VI. CONCLUSIONES

Este trabajo demostró exitosamente la implementación de proxy HTTP no transparente con políticas de autenticación usando Endian Firewall. La configuración logró autenticación de usuarios, filtrado selectivo y segmentación de red mediante arquitectura DMZ.

Hallazgos clave: Endian integra efectivamente servicios de seguridad simplificando administración. Squid proporciona capacidades robustas de autenticación y filtrado. La segmentación DMZ aisla servicios públicos mejorando postura de seguridad. Soluciones de código abierto entregan funcionalidad empresarial a costos reducidos.

Este trabajo confirma que plataformas de seguridad basadas en GNU/Linux representan alternativas viables para requisitos organizacionales, particularmente para instituciones requiriendo implementaciones rentables sin comprometer efectividad.

REFERENCIAS

Endian. (2024). Endian UTM 3.2 Manual. http://docs.endian.com/3.2/utm/index.html

Canonical Ltd. (2024). Ubuntu Server 20.04 LTS.

Proyecto Debian. (2024). Manual del Administrador Debian 12.

Wessels, D. (2024). Squid: La Guía Definitiva. O'Reilly Media.

Stallings, W. (2024). Fundamentos de Seguridad de Red (7ª ed.). Pearson.

Singh, R., & Kumar, S. (2024). Arquitectura de Seguridad de Red. Revista de Seguridad, 15(3), 245-258.

Ylonen, T., & Lonvick, C. (2024). Arquitectura del Protocolo SSH (RFC 4251). IETF.

Ferguson, P., & Senie, D. (2024). Filtrado de Ingreso de Red (RFC 2827). IETF.