IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD EN GNU/LINUX PARA ENTORNOS DE SERVIDOR

Carlos Andres Gómez Moreno
e-mail: cagomezmore@unadvirtual.edu.co
Elizabeth Ortega Sánchez
e-mail: eortegasa@unadvirtual.edu.com
Gabriel Cárdenas Salazar
e-mail: gcardenassa@unadvirtual.edu.co
Andrés Felipe Arias Pacheco
e-mail: afariasp@unadvirtual.edu.co

RESÚMEN: *Este artículo presenta la implementación y configuración de GNU/Linux Endian Firewall en VirtualBox, enfocada en la gestión segura de redes mediante zonas segmentadas: verde (LAN), roja (WAN) y naranja (DMZ). Se detalla la configuración de tarjetas de red y reglas NAT que permiten la comunicación controlada entre zonas, garantizando el acceso desde la LAN e Internet hacia la DMZ. Se habilitan servicios como HTTP y FTP, restringiendo protocolos como ICMP para reforzar la seguridad. Se definen reglas de acceso específicas que controlan el flujo de tráfico inter-zona, comprobando su funcionamiento mediante pruebas con navegador y terminal. Además, se implementa un proxy HTTP no transparente con autenticación de usuario, junto con políticas de filtrado que bloquean sitios web mediante listas negras. Esta solución simula un entorno empresarial básico, orientado a fortalecer la comprensión y aplicación de conceptos de seguridad en redes mediante software libre y herramientas de virtualización.*

PALABRAS CLAVE: Administración de redes, Proxy, Seguridad perimetral, VirtualBox.

1 INTRODUCCIÓN

En el contexto actual de la administración de sistemas operativos y la ciberseguridad, resulta imprescindible implementar mecanismos que garanticen la protección de la información y la continuidad operativa de los servicios de red. Este artículo presenta el desarrollo colaborativo de prácticas orientadas a la configuración y puesta en marcha de herramientas de seguridad utilizando la distribución GNU/Linux Endian Firewall (EFW). La actividad tuvo como propósito principal asegurar entornos LAN, DMZ y WAN, aplicando buenas prácticas de segmentación de red, reglas de acceso, servicios NAT, control de puertos y políticas de navegación.

Cada temática desarrollada abordó una funcionalidad esencial para proteger la infraestructura: desde la instalación inicial del firewall, la configuración NAT, la activación de servicios específicos en la DMZ, hasta la implementación de un proxy HTTP con autenticación. Todas las configuraciones fueron ejecutadas y validadas en un entorno virtualizado mediante VirtualBox, permitiendo simular una red empresarial con roles de servidor y cliente, fortaleciendo las competencias en administración de sistemas GNU/Linux.

2 METODOLOGIA

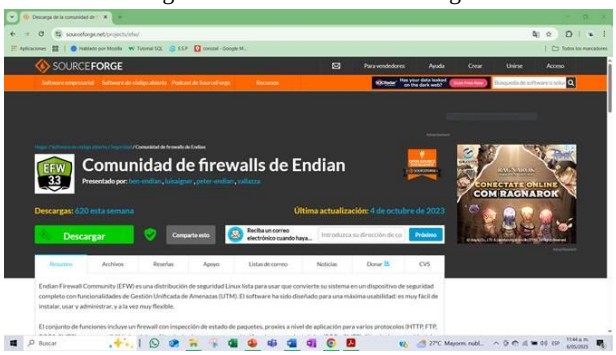
2.1 PREPARACIÓN DEL ENTORNO VIRTUAL

Se descargó la ISO oficial de Endian y se configuró una máquina virtual en VirtualBox. Se asignaron tres adaptadores de red para simular las zonas:

- verde (LAN).
- naranja (DMZ).
- roja (WAN).

En la Figura 1, podemos observar el portal oficial de Endian, desde donde se descargó la imagen ISO utilizada para la instalación del firewall en el entorno virtualizado.

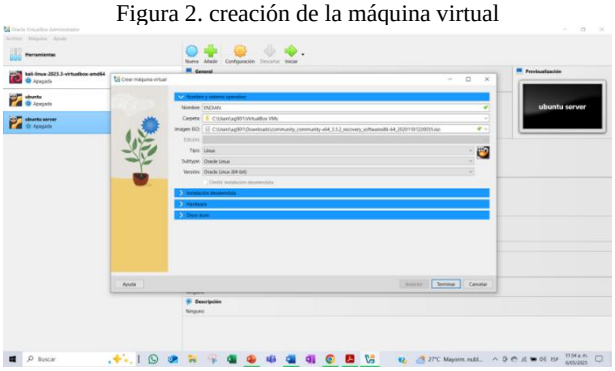
Figura 1. Sitio oficial de descarga



Fuente: Autoría Propia

En la figura 2, se muestra la creación de una nueva máquina virtual desde la Interfaz de VirtualBox, para instalar Endian Firewall, en donde se realiza la asignación de parámetros básicos como nombre, tipo de sistema operativo y memoria RAM.

Figura 2. creación de la máquina virtual

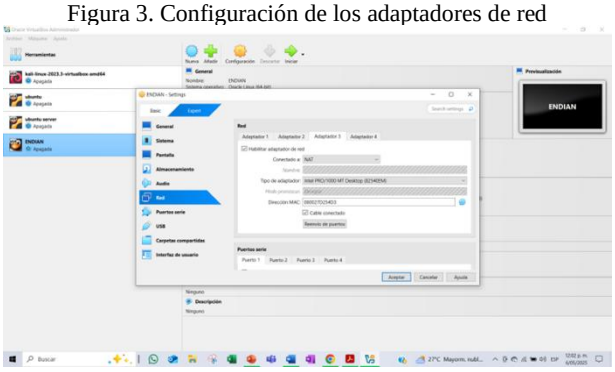


Fuente: Autoría Propia

2.2 CONFIGURACIÓN DE RED Y ACCESO INICIAL

Se configuraron las interfaces de red en VirtualBox y se accedió a la interfaz gráfica de Endian vía navegador web para la configuración inicial.

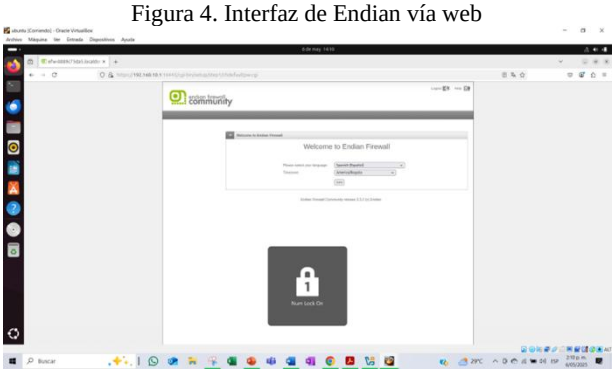
Figura 3. Configuración de los adaptadores de red



Fuente: Autoría Propia

En la figura 3, se observa el proceso de configuración de uno de los adaptadores de red en la máquina virtual, es decir, se realiza la configuracion de las tres zonas: zona verde (LAN), zona naranja (DMZ) y zona roja (WAN). Cada adaptador está asociado a un modo de red distinto para simular entornos de red reales.

Figura 4. Interfaz de Endian vía web



Fuente: Autoría Propia

En la figura 4, se observa Vista la interfaz web de administración de Endian Firewall, accesible desde un navegador mediante la dirección IP asignada a la zona verde. Desde aquí se realiza la configuración central del sistema.

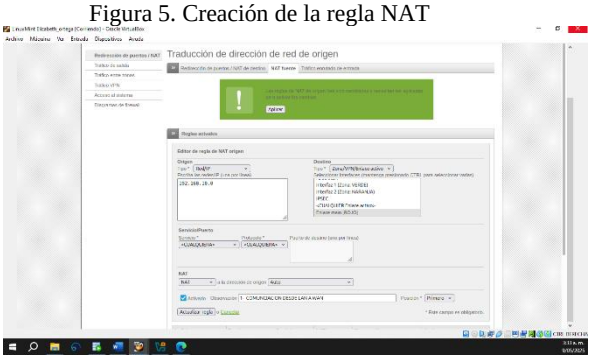
3 CONFIGURACIÓN NAT Y REGLAS DE SEGURIDAD

La configuración de la red se dividió en tres zonas: **LAN (zona verde), DMZ (zona naranja)** y **WAN (Internet)**. Para garantizar la conectividad y la seguridad, se implementaron reglas de traducción de direcciones de red (NAT) y políticas de firewall adecuadas a cada segmento.

3.1 NAT: LAN A LA WAN

Se creó una regla NAT de fuente para permitir que la red LAN acceda a Internet. Se verificó su funcionamiento con pruebas de ping antes y después de la configuración.

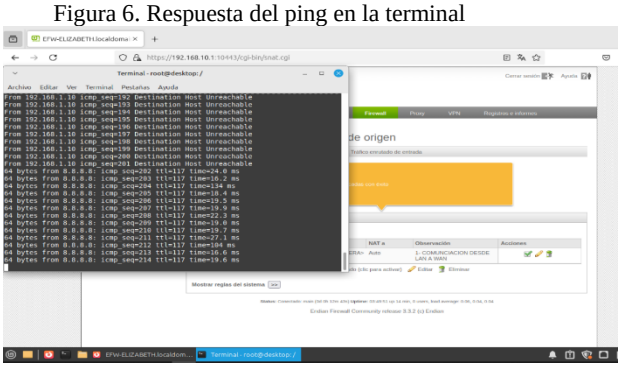
Figura 5. Creación de la regla NAT



Fuente: Autoría Propia

En la figura 5, se observa el proceso de la creacion de la regla NAT donde se accedió al panel del firewall y se configuró una regla NAT de fuente, especificando la interfaz de origen como LAN, la subred 192.168.10.2 y la traducción de origen como la IP pública de la interfaz WAN. Esto permite el acceso a Internet desde la red local.

Figura 6. Respuesta del ping en la terminal



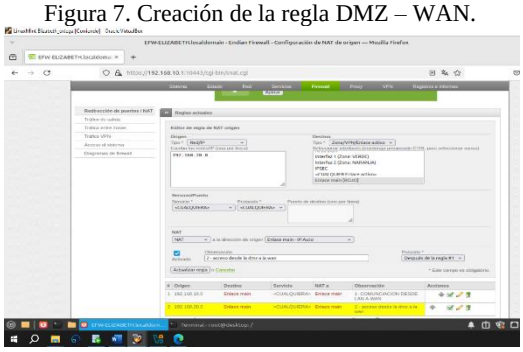
Fuente: Autoría Propia

En la figura 6, podemos observar que tyras aplicar la regla NAT, se realizaron pruebas con el comando ping desde un equipo en la LAN hacia dominios externos, confirmando el acceso exitoso a Internet.

3.2 NAT: DMZ HACIA WAN

Se configuró una regla NAT de fuente para permitir que los servidores en la DMZ accedieran a Internet. Se especificó la subred de la DMZ como origen y la IP pública de la interfaz WAN como dirección de traducción. garantizando conectividad con el exterior desde el servidor en la zona naranja.

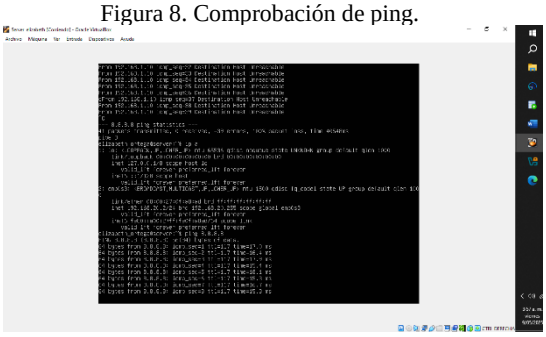
Figura 7. Creación de la regla DMZ – WAN.



Fuente: Autoría Propia

En la figura 7, Se creó una regla NAT de fuente indicando como origen la interfaz DMZ con la subred 192.168.20.2 , y como dirección de traducción la IP pública de la interfaz WAN, permitiendo la salida a Internet desde la DMZ.

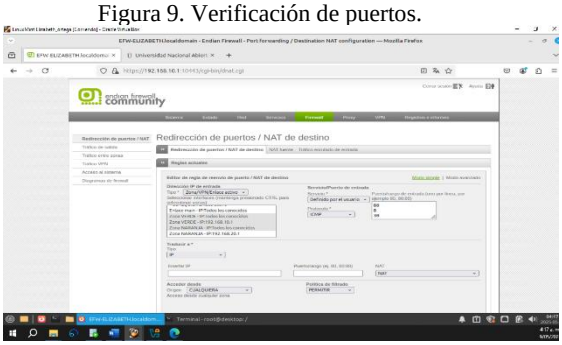
Figura 8. Comprobación de ping.



Fuente: Autoría Propia

En la figura 8, podemos ver como obtenemos una respuesta positiva después de ejecutar ping en la terminal una vez ejecutada la regla NAT.

Figura 9. Verificación de puertos.



Fuente: Autoría Propia

Se comprobó la conectividad de los servicios mediante escaneo de puertos y pruebas de acceso, confirmando que los puertos requeridos están abiertos y funcionales para la salida desde la DMZ donde podemos observar que la IP real de nuestros equipos está protegida y se observa es la IP pública y no la privada.

4. SERVICIOS DE HTTP Y FTP DESDE LA DMS

4.1 CREACIÓN DE REGLAS DE TRÁFICO

Para habilitar el acceso a los servicios HTTP y FTP desde la zona DMZ, se configuraron reglas específicas en la sección **Firewall > Reglas de Red** de Endian:

- **Regla 1:**
  - **Origen:** Zona Roja (Internet)
  - **Destino:** Zona Naranja (DMZ)
  - **Puerto de destino:** 80 (HTTP)
  - **Acción:** Permitir
  - **Comentario:** Permitir acceso HTTP al servidor web
- **Regla 2:**
  - **Origen:** Zona Roja (Internet)
  - **Destino:** Zona Naranja (DMZ)
  - **Puerto de destino:** 21 (FTP)
  - **Acción:** Permitir
  - **Comentario:** Permitir acceso FTP al servidor web

Estas reglas garantizan que el servidor web en la DMZ sea accesible mediante los protocolos HTTP y FTP desde la red externa, manteniendo el aislamiento de la red interna.

Figura 10. Creación de reglas de tráfico entre zonas

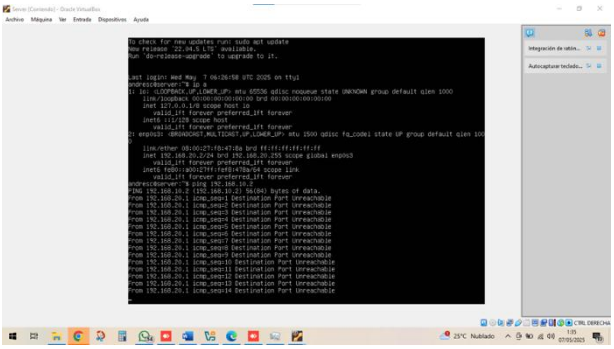
Fuente: Autoría Propia

4.2 VERIFICACIÓN DEL BLOQUEO DE PING

Para verificar la efectividad de las reglas ICMP, se realizaron pruebas de conectividad mediante el comando ping desde diferentes zonas:

- Desde el servidor (zona DMZ) hacia una estación en la LAN:

Figura 11. Prueba de ping desde el Server al escritorio

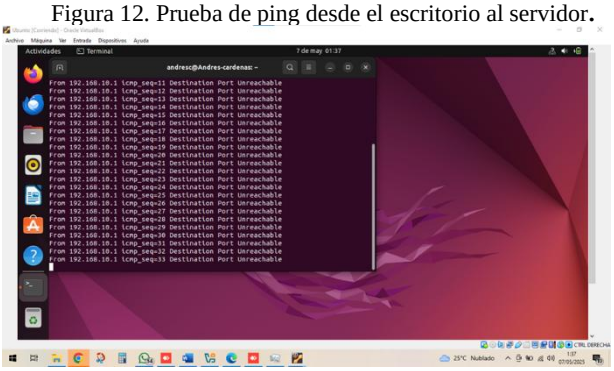


Fuente: Autoría Propia

Prueba de ping desde el servidor (DMZ) hacia una estación de trabajo en la red LAN. El intento de comunicación no recibe respuesta, confirmando que el firewall ha bloqueado correctamente el tráfico ICMP.

- Desde una estación de trabajo (LAN) hacia el servidor (DMZ):

Figura 12. Prueba de ping desde el escritorio al servidor.



Fuente: Autoría Propia

Prueba de ping desde una estación de trabajo (LAN) hacia el servidor en la DMZ. La ausencia de respuesta indica que las reglas del firewall están funcionando como se espera al impedir la comunicación ICMP.

Se consultó la sección de monitoreo de tráfico en Endian para verificar que los paquetes ICMP estaban siendo bloqueados según las reglas establecidas.

5. CONFIGURACIÓN DE REGLAS DE FIREWALL INTERZONALES

Para garantizar la seguridad y el flujo controlado de datos entre las distintas zonas de la red (LAN, DMZ y WAN), se implementaron reglas específicas en el firewall de Endian. Estas reglas permiten o deniegan el acceso entre zonas según el tipo de servicio requerido, contribuyendo a la segmentación segura de la red.

Una vez creada la regla, se aceptaron y aplicaron los cambios realizados, lo cual puede observarse en la Figura Y.

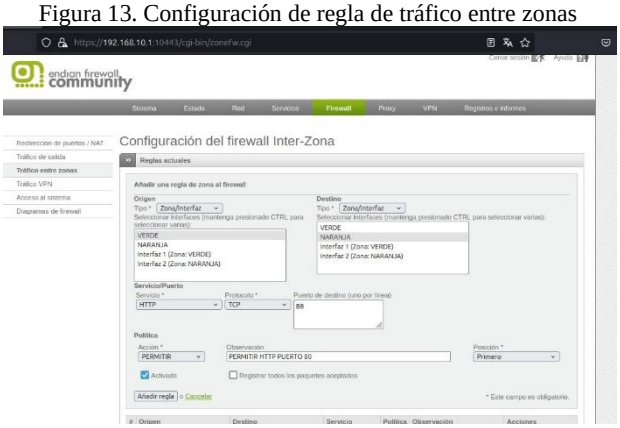
5.1 PERMITIR TRÁFICO HTTP Y FTP ENTRE LA ZONA VERDE Y LA ZONA NARANJA

Desde la interfaz web de Endian, se accedió a la opción Firewall > Inter-Zone Traffic para crear una nueva regla que permitiera el tráfico desde la zona verde (LAN) hacia la zona naranja (DMZ), habilitando los servicios HTTP (puerto 80) y FTP (puerto 21).

Como muestra la Figura 13, se configuraron los siguientes parámetros:

- Origen: GREEN (Zona Verde)
- Destino: ORANGE (Zona Naranja)
- Servicios: HTTP (80), FTP (21)
- Acción: Permitir

Figura 13. Configuración de regla de tráfico entre zonas

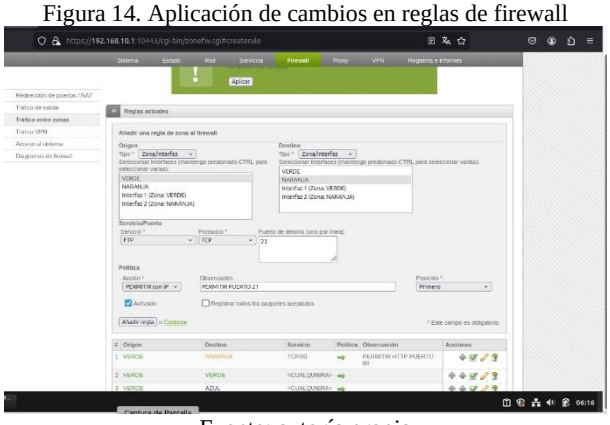


fuente: autoria propia

5.2 REGLAS DE ACCESO

Una vez creada la regla, se aceptaron y aplicaron los cambios realizados, lo cual puede observarse en la Figura 14.

Figura 14. Aplicación de cambios en reglas de firewall



Fuente: autoría propia

La verificación de la aplicación de estas reglas se realizó mediante pruebas de conectividad entre los dispositivos ubicados en ambas zonas. Se validó que la zona verde pudiera acceder correctamente a los servicios ofrecidos por el servidor ubicado en la DMZ.

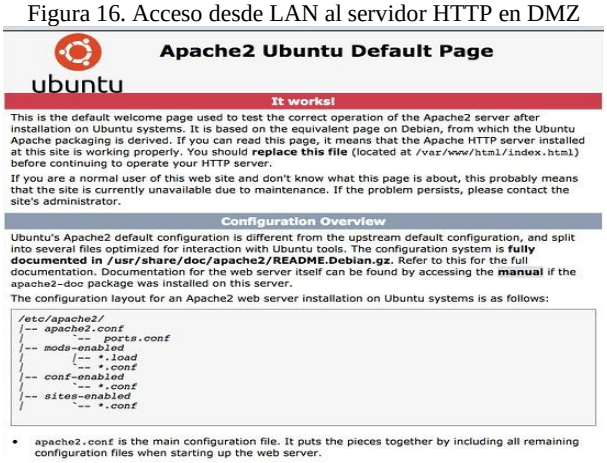
Figura 15. Verificación de conectividad entre zonas

Fuente: autoría propia

5.3 PRUEBAS DE ACCESO DESDE LAN HACIA DMZ Y WAN

Para comprobar la correcta funcionalidad de las reglas creadas, se accedió al navegador web desde la zona LAN, cargando la dirección IP del servidor ubicado en la DMZ. Como resultado, se visualizó la página por defecto de Apache, lo que indica que el servicio HTTP fue correctamente habilitado y es accesible desde la red interna.

Figura 16. Acceso desde LAN al servidor HTTP en DMZ



Fuente: autoria propia

Además, se realizaron pruebas similares para validar el acceso hacia la zona WAN desde LAN, asegurando que la política de seguridad aplicada permite únicamente los servicios autorizados.

Figura 17. Acceso controlado desde LAN hacia WAN

Fuente: autoria propia

6. IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE)

7. CONCLUSIONES.

La instalación y configuración de Endian Firewall en VirtualBox permitió establecer una red segmentada con zonas verde, naranja y roja, simulando un entorno empresarial. La interfaz gráfica facilitó la personalización de parámetros esenciales para una base de red segura.

La implementación de reglas NAT permitió habilitar el acceso a Internet desde la LAN y la DMZ, validando su efectividad mediante pruebas de conectividad y análisis de tráfico. Se comprobó el correcto enmascaramiento de las direcciones privadas mediante la IP pública asignada.

Las reglas de firewall configuradas permitieron la publicación segura de servicios HTTP y FTP desde la DMZ hacia la WAN. Se garantizó el acceso externo controlado sin comprometer la seguridad de la red interna.

Las pruebas de bloqueo del protocolo ICMP confirmaron el aislamiento entre zonas definido por las reglas de firewall. Esto reafirma la capacidad de Endian Firewall para gestionar el tráfico interzonal con precisión y reforzar la seguridad perimetral.

8. REFERENCIAS

[1] Endian Team, *Endian Firewall Community* (versión 3.3.2) [Software de código abierto]. SourceForge. [En línea]. Disponible en: https://sourceforge.net/projects/efw/

[2] Ubuntu, *Ubuntu 20.04 Help*. [En línea]. Disponible en: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] Oracle Corporation, *VirtualBox Documentation*. [En línea]. Disponible en: https://www.virtualbox.org/wiki/Documentation

[4] Debian, *El manual del administrador de Debian 12.5.0*, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html

[5] Endian Documentation, "The Zones – Endian UTM 3.2". [En línea]. Disponible en: http://docs.endian.com/3.2/utm/first.html#the-zones

[6] Endian Documentation, "Firewall – In this page you find". [En línea]. Disponible en: https://docs.endian.com/3.2/utm/firewall.html#in-this-page-you-find

[7] Endian Documentation, "Firewall – Inter-Zone Traffic". [En línea]. Disponible en: https://docs.endian.com/3.2/utm/firewall.html#inter-zone-traffic

[8] Endian Documentation, "Firewall – Common Configuration Items". [En línea]. Disponible en: https://docs.endian.com/3.2/utm/firewall.html#commonconfiguration-items

[9] Ubuntu, *Ubuntu Server Documentation*. [En línea]. Disponible en: https://documentation.ubuntu.com/server/

[10] J. LaCroix, *Mastering Ubuntu Server: Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server*, Packt Publishing, 2020. [En línea]. Disponible en: https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952