PROYECTO FINAL

1. OBJETIVOS

1.1. Objetivo General

Diseñar e implementar una infraestructura de red segmentada y segura, aplicando los conceptos adquiridos en la clase magistral y de laboratorio, con el fin de optimizar la comunicación entre dispositivos, garantizar el control de acceso y supervisar el tráfico de red.

1.2. Objetivos Específicos

- Configurar una intranet segmentada en VLANs para separar y organizar servicios internos.
- Implementar controles de acceso basado en direcciones IP y MAC.
- Configurar un proxy transparente que filtre y restrinja el acceso a sitios web en internet.
- Desarrollar un balanceador de carga con failover para administrar eficientemente los enlaces a Internet.
- Implementar un sistema de monitoreo de red que permita supervisar el uso de recursos y enlaces.
- Establecer una VPN que garantice el acceso remoto seguro a los servicios internos autorizados.

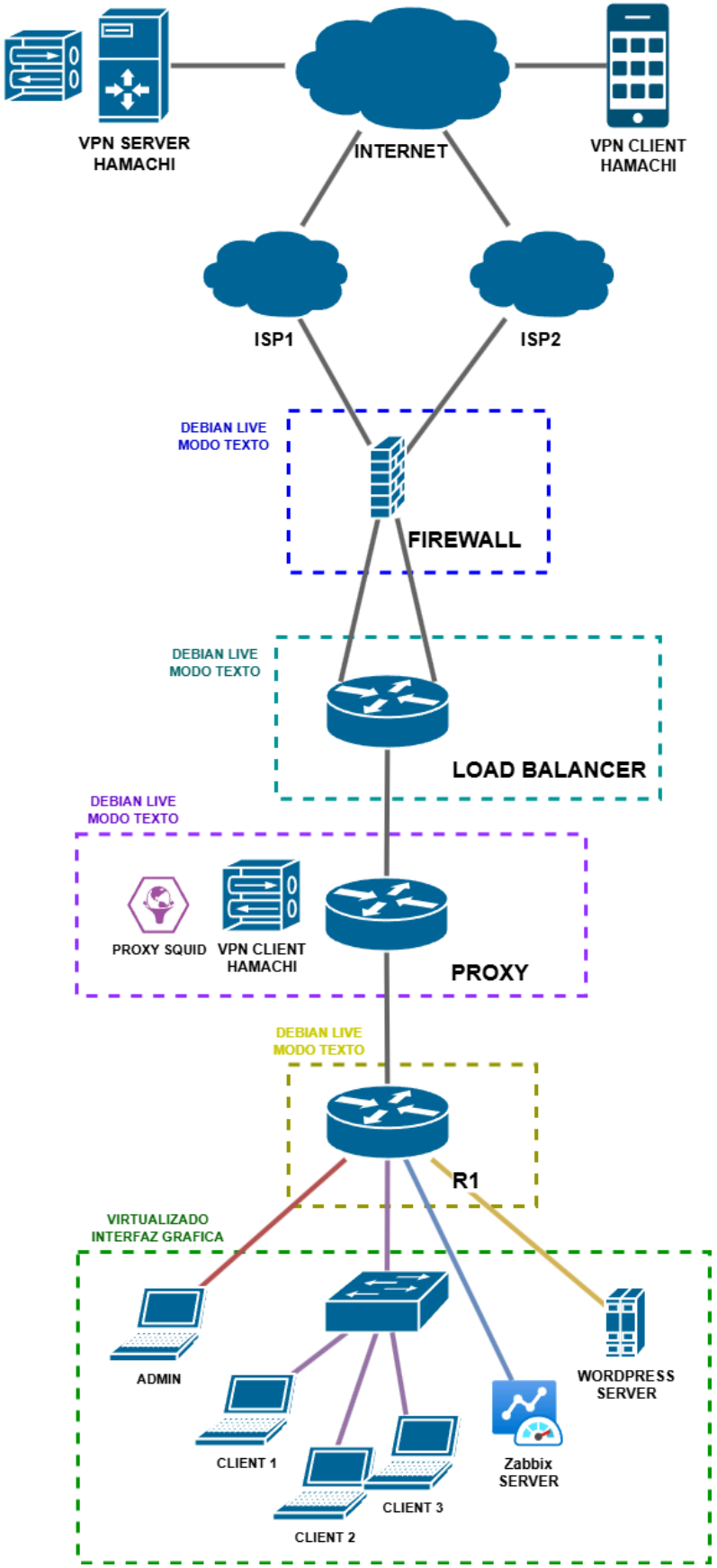
2. DESCRIPCIÓN

La Speedwagon Foundation ha decidido modernizar su infraestructura de red y ha decidido volver a contar con su equipo de trabajo dado el éxito del proyecto anterior. Se han contratado dos diferentes proveedores de servicios de Internet (ISP) con el fin de garantizar alta disponibilidad, redundancia y balanceo de carga.

Además, busca implementar una intranet corporativa, con un sistema de seguridad centralizado que permita controlar de forma granular el acceso de clientes y administradores tanto a los recursos internos como al Internet.

La organización quiere exponer su servidor interno únicamente a clientes autorizados mediante el uso de VPN y reglas de firewall personalizadas, manteniendo el resto inaccesible desde el exterior.

2.1. Diagrama general de la arquitectura de red a implementar



3. ELEMENTOS DE LA ARQUITECTURA

3.1. Intranet

La intranet deberá estar segmentada en 4 VLANs:

- Administración
- Clientes
- Gestión (Zabbix)
- Servidor WordPress

Solo el administrador y los clientes tendrán interfaz gráfica. Para Zabbix y WordPress se utilizará Linux en modo texto.

3.2. Router-R1

En él se realizará la asignación de VLANs. Además se encargará del enrutamiento interno de la intranet. Implementará reglas de acceso con la política “todo cerrado”.

Accesos permitidos:

- Solo el administrador puede acceder a Zabbix y a la configuración del servidor WordPress.
- Desde el administrador se debe poder configurar toda infraestructura de red.
- Los clientes pueden acceder al servidor WordPress únicamente en modo lectura/uso de forma predeterminada.

Se puede gestionar el router mediante los archivos:

VLANs.conf

```
#ID_VLAN    #INTERFACES
10          eth0 eth1 eth2
```

access.mac

```
A1:B4:C5:C1:DD:3E
A1:B4:C5:C1:DD:3F
A1:B4:C5:C1:DD:40
```

access.ip

```
192.168.0.1
192.168.0.2
192.168.0.3
```

Solo las direcciones MAC e IP que se encuentran en los archivos tendrán acceso a internet.

3.3. Proxy y Cliente VPN

Debe instalarse y configurar proxy Squid en modo transparente, de forma que no sea necesario modificar la configuración de los navegadores ni de los sistemas operativos clientes.

El proxy aplicará el siguiente filtrado:

- **Bloquear**: sitios pornográficos y redes sociales.
- **Permitir**: Sitios gubernamentales de Guatemala y bancos de Guatemala

También deberá instalarse un cliente VPN Hamachi, que permita exponer el servidor WordPress de la intranet hacia el exterior. Solo clientes autenticados en la VPN podrán acceder al WordPress.

3.4. Balanceador de Carga

Este equipo recibirá conexión transparente de los dos enlaces de los ISPs. Debe implementar un sistema de **failover** automático en caso de caída y/o recuperación de un enlace.
El balanceo de carga dependerá de varios archivos de configuración:

bandwidth.conf

Define el ancho de banda disponible de cada ISP (en Kbps).

```
#<ISP>, <UP>, <DW>
ISP1, 512, 512
ISP2, 1000, 1000
```

LB_rules.conf

Define reglas específicas de salida hacia un ISP en particular (ISP1 o ISP2) . Por defecto se aplicarán las siguientes reglas:

- ISP1: Tráfico http y https
- ISP2: Resto del tráfico

```
#<ip_origen>, <puertos>, <protocolo>, <ISP_salida>
192.168.1.1, [443, 80], TCP, ISP1
192.168.1.2, [22], TCP, ISP2
```

El balanceador deberá también enviar métricas de ancho de banda de cada ISP a **Zabbix** para su monitoreo. Solo el administrador puede acceder al dashboard de Zabbix.

3.5. Firewall

El firewall cuenta con 4 interfaces de red, conectado entre los ISPs y el balanceador de carga. Funciona de manera transparente, filtrando únicamente el tráfico entrante antes de llegar al servidor:

ingress.rules

```
#<origen>, <destino>, <puertos>, <protocolo>
0.0.0.0, 20.1.56.80,[80,443], TCP
```

3.6. VPN

Se debe configurar un servidor VPN desde la página oficial de Hamachi . Se deberá además configurar un cliente móvil (Android o iOS). El acceso al servidor WordPress puede hacerse directamente desde la VPN configurada.

4. RESTRICCIONES

- Grupos de 5 integrantes, cada persona tiene un rol.
    - Solo el administrador y los clientes virtualizados deben tener interfaz gráfica. (Se recomienda QEMU/KVM con Virt-Manager).
    - Toda la topología debe ser implementada con Debian en modo texto ya sea utilizando la versión live en USB o realizando una instalación completa.
- Uso de Linux obligatorio
- Configuraciones PROPIAS en modo texto, no interfaz gráfica.
- No se permite el uso de DHCP para configuración de interfaces.
- Las copias serán anuladas y reportadas.

5. ENTREGA

La fecha de entrega es el día martes **14 de octubre de 2025 a las 15:00 horas**. En la plataforma classroom deberá adjuntar el link al repositorio de GitHub del proyecto. El respiratorio deberá incluir:

- Scripts de configuración utilizados en cada componente de su arquitectura bien organizados.
- Documentación completa en formato PDF o Markdown
    - Diseño de la arquitectura de red
    - Explicación de su solución y los elementos que componen su arquitectura.