**Requerimientos Infraestructura**

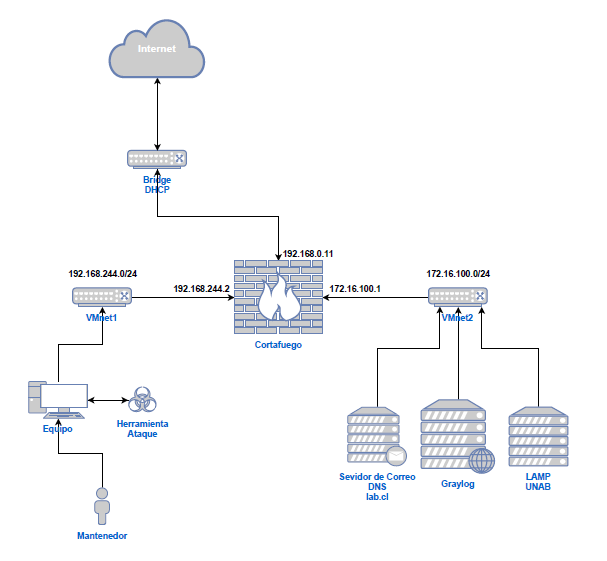
1. **Objetivo de Requerimientos**

El objetivo de estos “Requerimientos de Infraestructura” es contar un laboratorio que cumpla con la operatividad y sostenimiento del proyecto titulado como “**Propuesta de Infraestructura TI de bajo costo para proteger una RED CORPORATIVA de micro y pequeñas empresas**”.

Se hace presente que estos requerimientos están basados y estimados en una red de pequeña y mediana empresa (30 dispositivos que reporten al correlacionador) para que el sistema funcione de manera optima, en caso se requiera el ingreso de nuevos dispositivos, se debe realizar una nueva evaluación de los requerimientos.

1. **Infraestructura propuesta:**

A continuación, se detalla el Core de la infraestructura propuesta para este proyecto.



**Figura 1: Infraestructura propuesta**

La infraestructura que se presenta y con la cual se detectarán ataques informáticos dentro de la red, esta compuesta por:

1. Correlacionador de eventos Open Source (Graylog).
2. Cortafuegos Open Source (pfSense).
3. Servidor de correo Open Source (Postfix - Dovecot).
4. Servidor DNS (Bind).
5. Herramienta generadora de ataques.
6. Modulo de detección y categorización de ataques.
7. **Consideraciones.**

Respecto a la infraestructura propuesta en la Figura 1, se deben tener presente siguientes aspectos:

1. La Figura 1 muestra el diagrama general para que el sistema opere en forma optima, partiendo desde cero en una red.
2. En el caso de que la red donde se implementara el sistema cuente con algunos de estos dispositivos, estos pueden utilizarse.
3. Se debe considerar que hay que tener dispositivos (input) para que reporten al correlacionador. En este punto lo importante es individualizar que dispositivos se configuraran para que reporten logs a nuestro correlacionador de eventos.
4. En estos requerimientos se incluirán algunos de los “inputs” para que comience a operar el sistema.
5. **Requerimientos:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Dispositivo | RAM | Storage | Core |
| 1 | Correlacionador de eventos Open Source, Graylog. | 8 Gb. | 200 Gb. | 6 |
| 2 | Cortafuegos Open Source (pfSense). | 4 Gb. | 60 Gb. | 2 |
| 3 | Servidor de correo Open Source (Postfix - Dovecot) y Servidor DNS. | 2 Gb. | 40 Gb. | 2 |
| 4 | Servidor LAMP (Linux, Apache, MySql, Php) | 2 Gb. | 40 Gb. | 2 |
| 5 | Equipo Atacante. | 2 Gb. | 40 Gb. | 2 |
| 6 | Equipo Monitoreo | 2 Gb. | 40 Gb. | 2 |
| 7 | Equipo Input 1 | 2 Gb. | 40 Gb. | 2 |
| 8 | Equipo Input 2 | 2 Gb. | 40 Gb. | 2 |
| 9 | Equipo Input 3 | 2 Gb. | 40 Gb. | 2 |
| 10 | Equipo Input 4 | 2 Gb. | 40 Gb. | 2 |
| 11 | Equipo Input 5 | 2 Gb. | 40 Gb. | 2 |
|  | | | | |
| Total Requerimientos | | 30 Gb. | 620 Gb. | 26 |

**Tabla 1: Detalle de requerimientos**

Respecto a estos requerimientos, es lo estimado para que el sistema funcione y opere de manera optima.

1. **Conclusión**

La infraestructura que se propone esta basada principalmente en la virtualización de maquinas, con el objetivo de minimizar los costos para la o las pymes que deseen implementar dicho sistema; ya que, si se utilizaran servidores dedicados para cada componente el costo se incrementaría bastante.