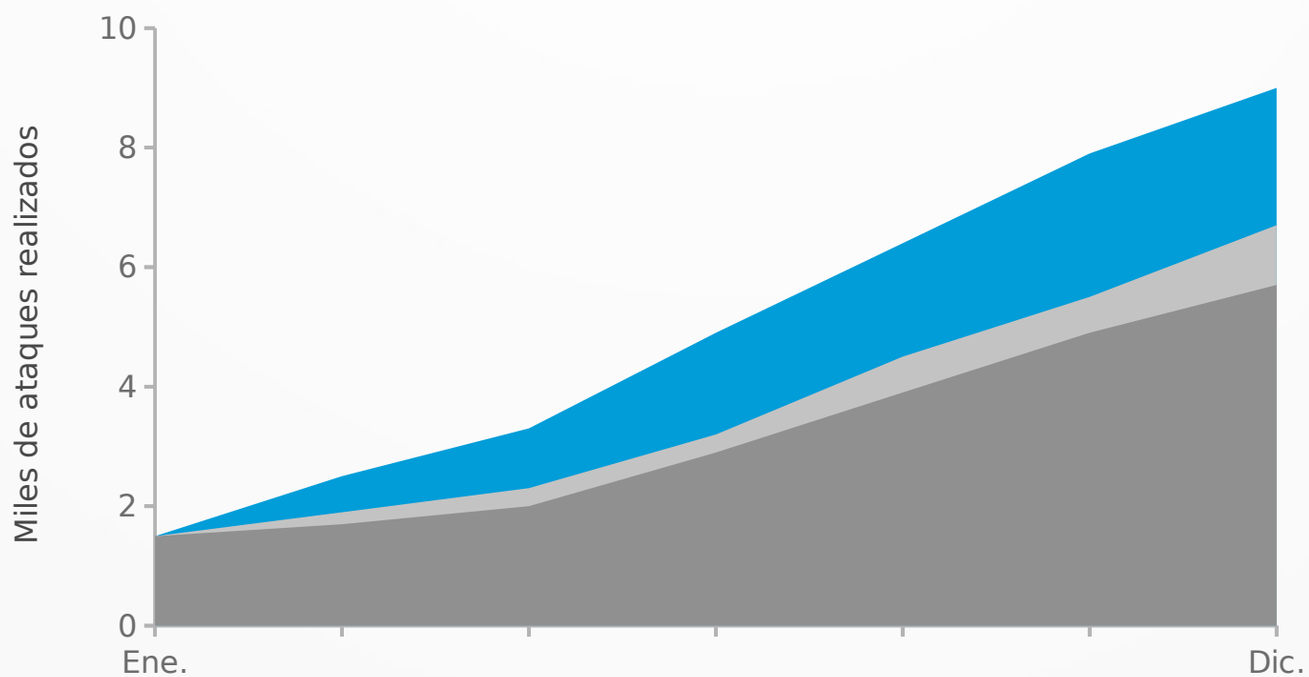
Honeypot

Un tarro de miel para los atacantes.

Seguridad hoy día

- Numero de ataques aumenta ↑ ↑ ↑
- Complejidad de los ataques ↑ ↑ ↑



Inspiración

孫子

“Conoce a tu enemigo y conócete a ti mismo; en cien batallas, nunca saldrás derrotado.” Sun Tzu, El arte de la guerra

¿Qué es un honeypot?

- Un Honeypot un sistema diseñado para analizar cómo los ciberdelincuentes emplean sus armas para intentar entrar en un sistema (analizan las vulnerabilidades) y alterar, copiar o destruir sus datos o la totalidad.

- Funciones: desviar atención, capturar nuevos virus/gusanos, formar perfiles, conocer nuevas vulnerabilidades.

Clasificación de honeypots:

Ambiente de Implementación:

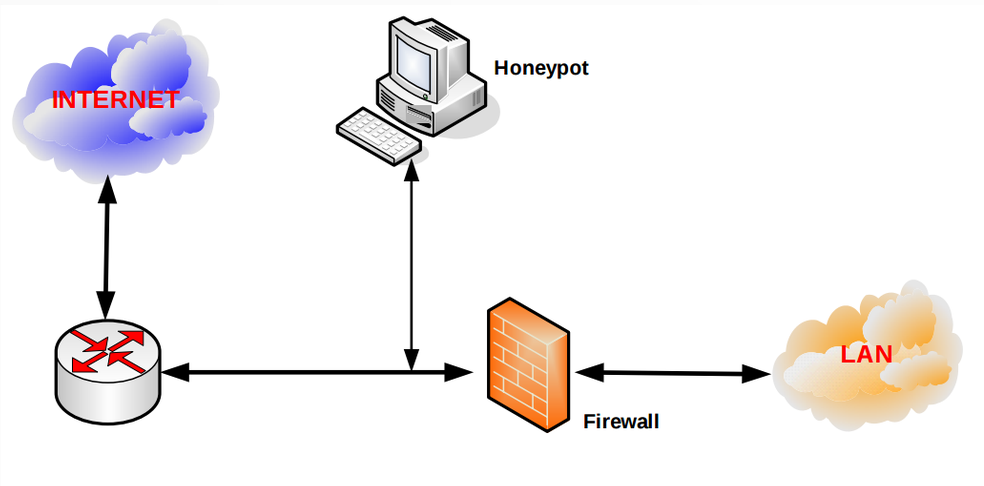
- Producción
- Investigación

Nivel de Interacción:

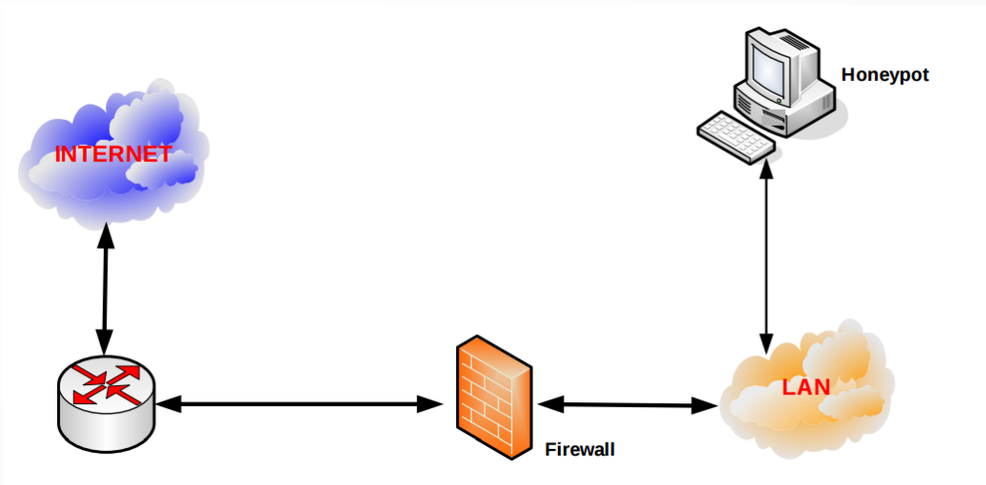
- Baja
- Alta

Ubicación de los honey

1) Antes del firewall

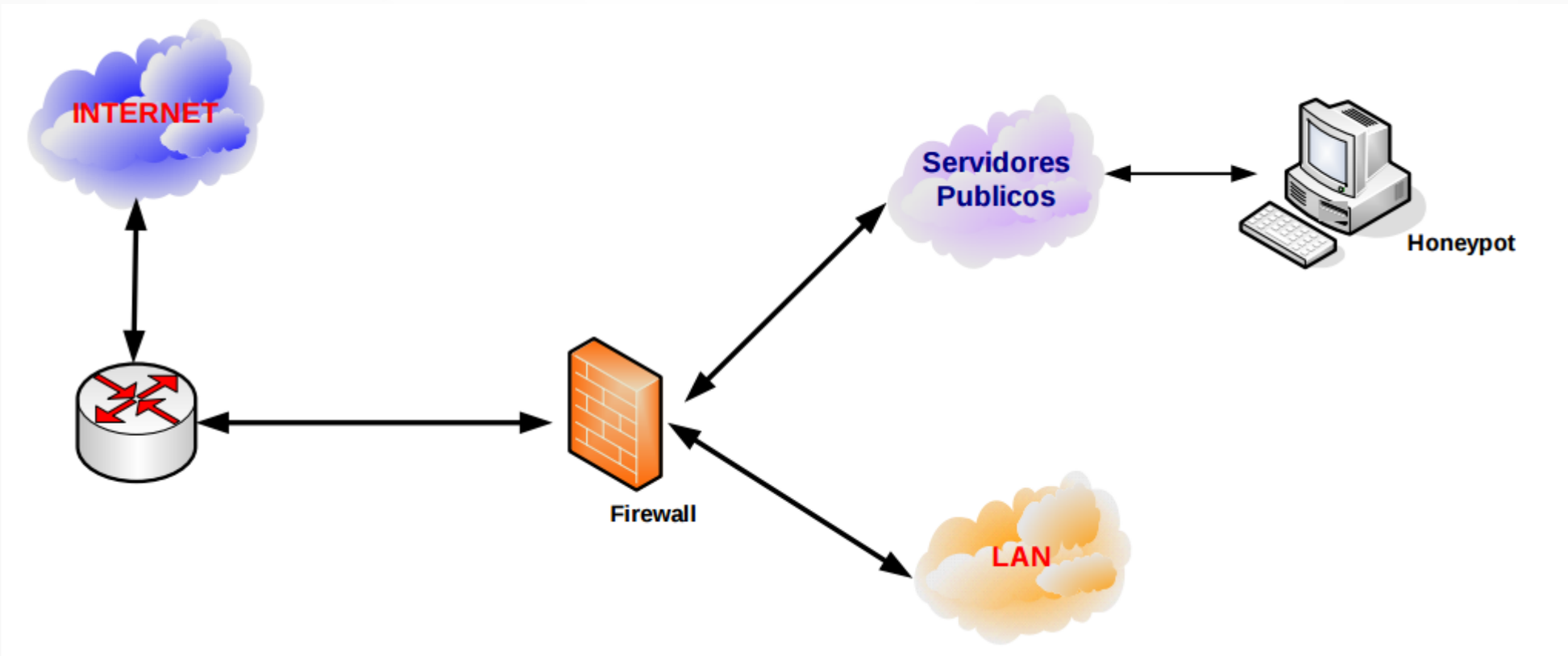


2) Detrás del firewall



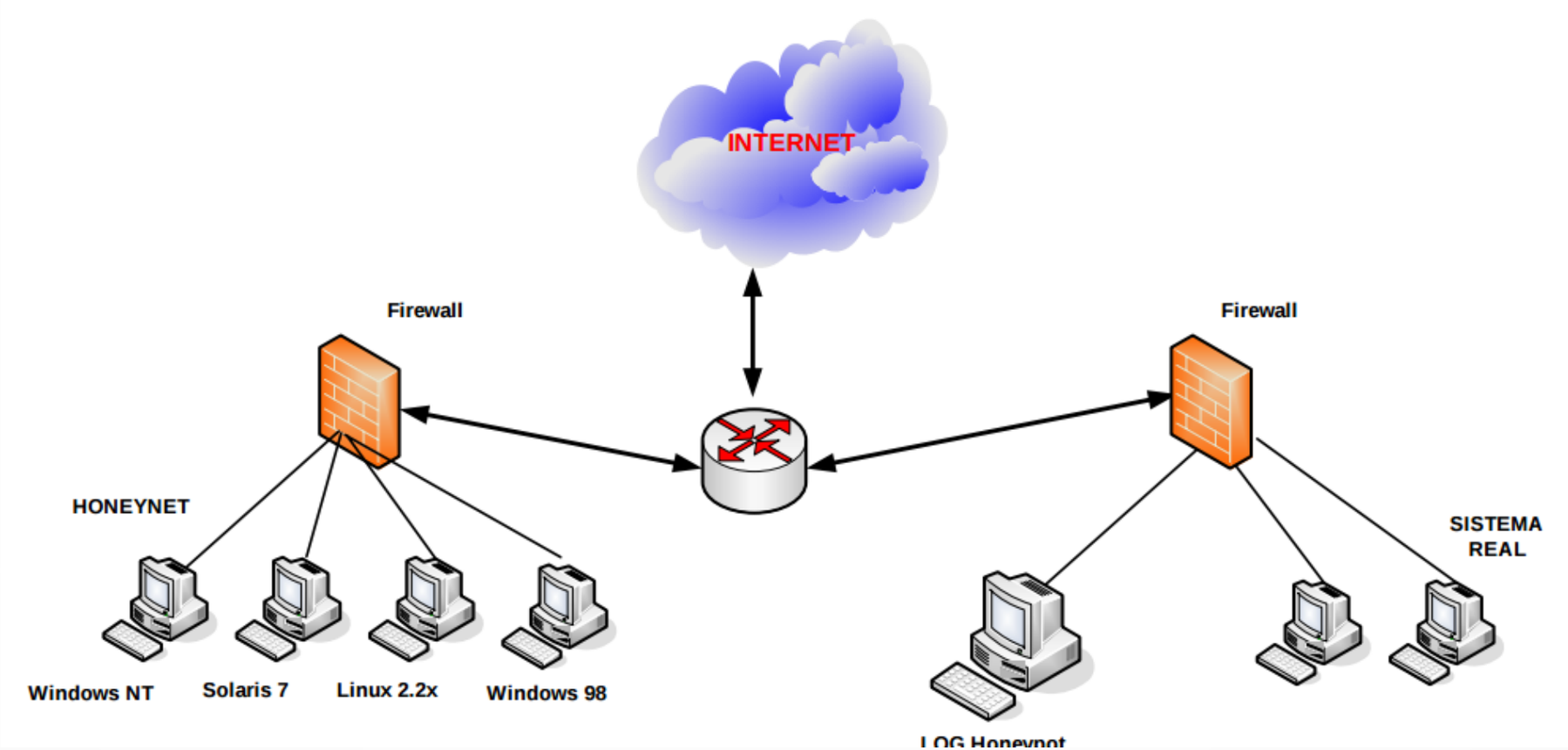
Ubicación de los honey

3) Zona desmilitarizada



HoneyNets

Zona desmilitarizada + Altamente interactivo



Usos reales

- NORSE
  - Empresa dedicada a la seguridad, ofrecen un producto hardware para filtrar conexiones a nuestra red y un mapa online de ataques.
  - http://map.norsecorp.com/
- The Honeynet Project
  - Organización dedicada a la investigación de los ataques en Internet usando honeypots.
  - http://www.honeynet.org/

Usos reales

- Capture-HPC
  - Cliente de alta interacción identifica los servidores maliciosos.
  - https://projects.honeynet.org/capture-hpc
- Google Hack Honeypot
  - Nuevo tipo de tráfico web malicioso: buscar los hackers del motor de búsqueda.
  - http://ghh.sourceforge.net

Usos reales

- HoneySink
  - Sinkholing es una técnica para supervisar y monitorear redes de ataques por bots.
  - https://www.aldeid.com/wiki/HoneySink
- HoneyStick
  - Herramienta de arranque por USB. Incluye honeywall y honeypots.
  - http://www.ukhoneynet.org/research/honeystick-howto/

Nuestro Honey

KIPPO

Es un honeypot de interacción media por SSH para recibir ataques por fuerza bruta captando la actividad del atacante por terminal. Desarrollado bajo Python y Twisted.

https://github.com/desaster/kippo