

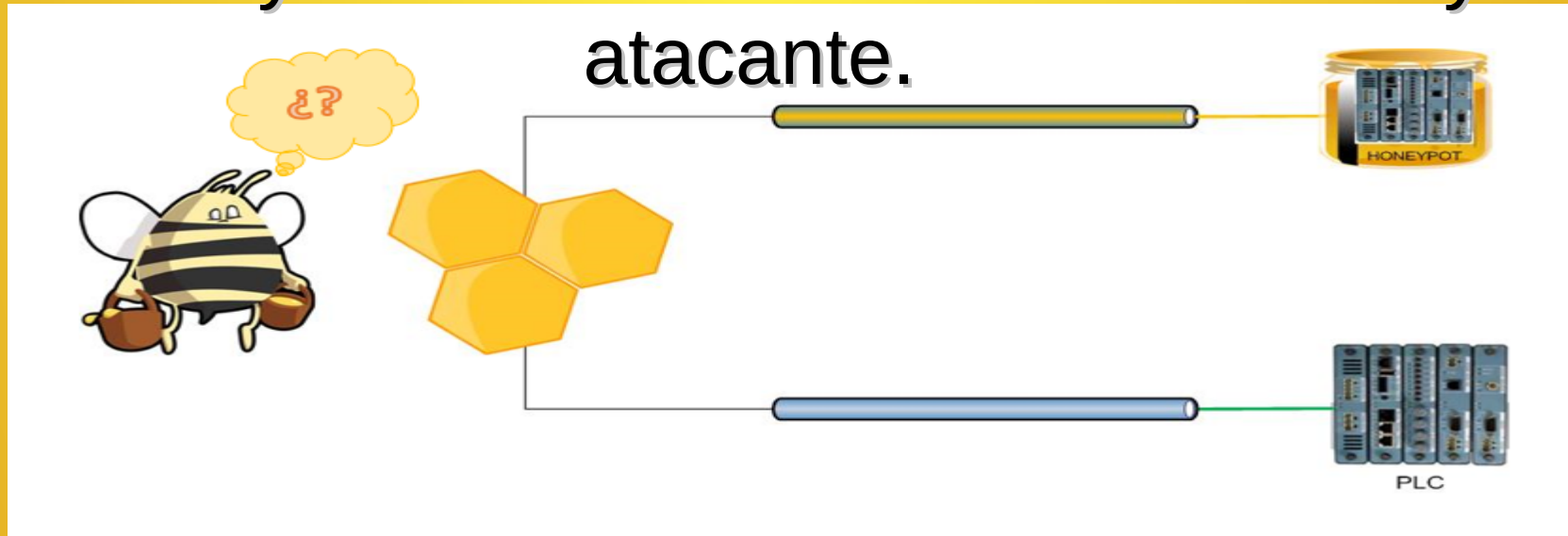


Honeypot

by : Jesús Ruiz Castellano

¿ Qué es ?

Un Honeypot, o señuelo, es una herramienta de la seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante.

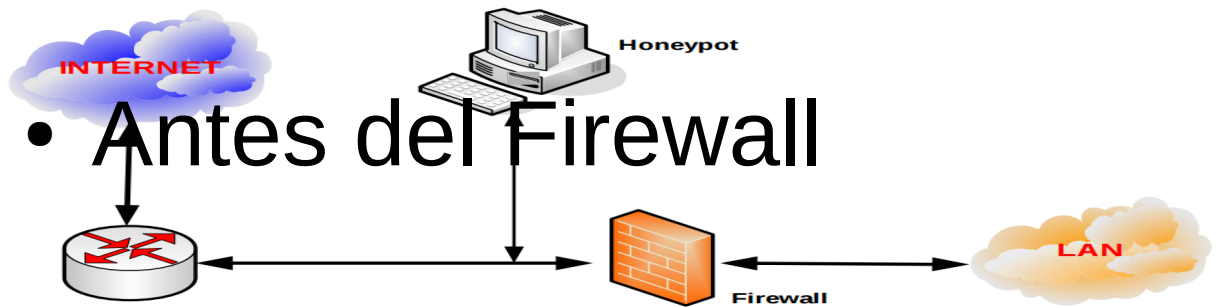


CLASIFICACION

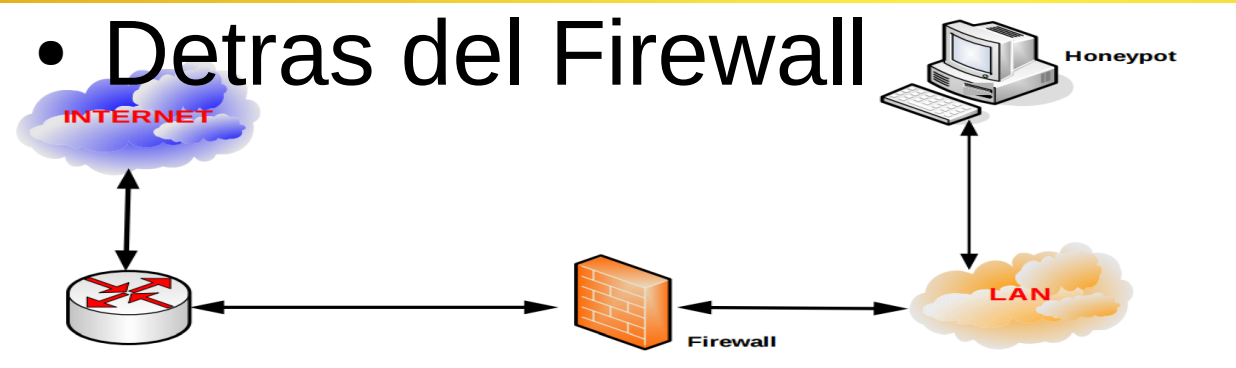
- Según su Ambiente de Implementación
 - Honeypots para la Producción
 - Honeypots para la Investigación
- Según su Nivel de Interacción
 - Honeypots de Baja Interacción
 - Honeypots de Alta Interacción

¿ Dónde ubicarlos ?

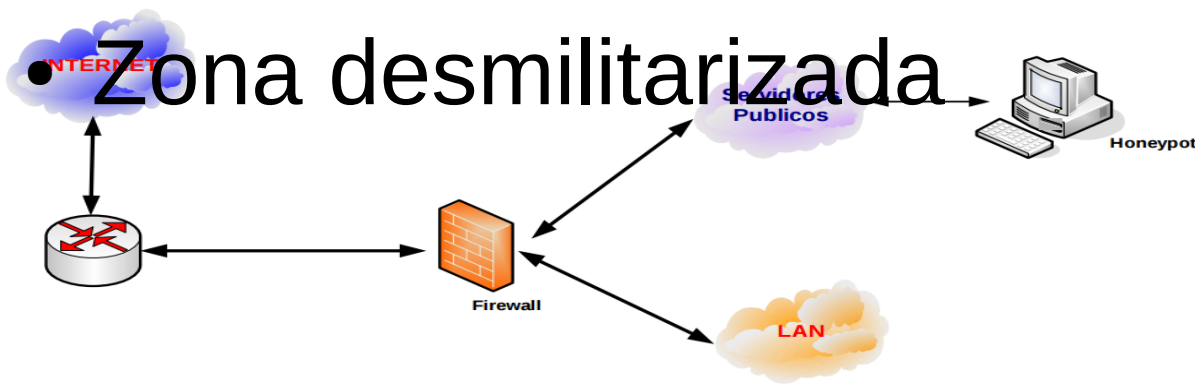
- Antes del Firewall



- Detrás del Firewall



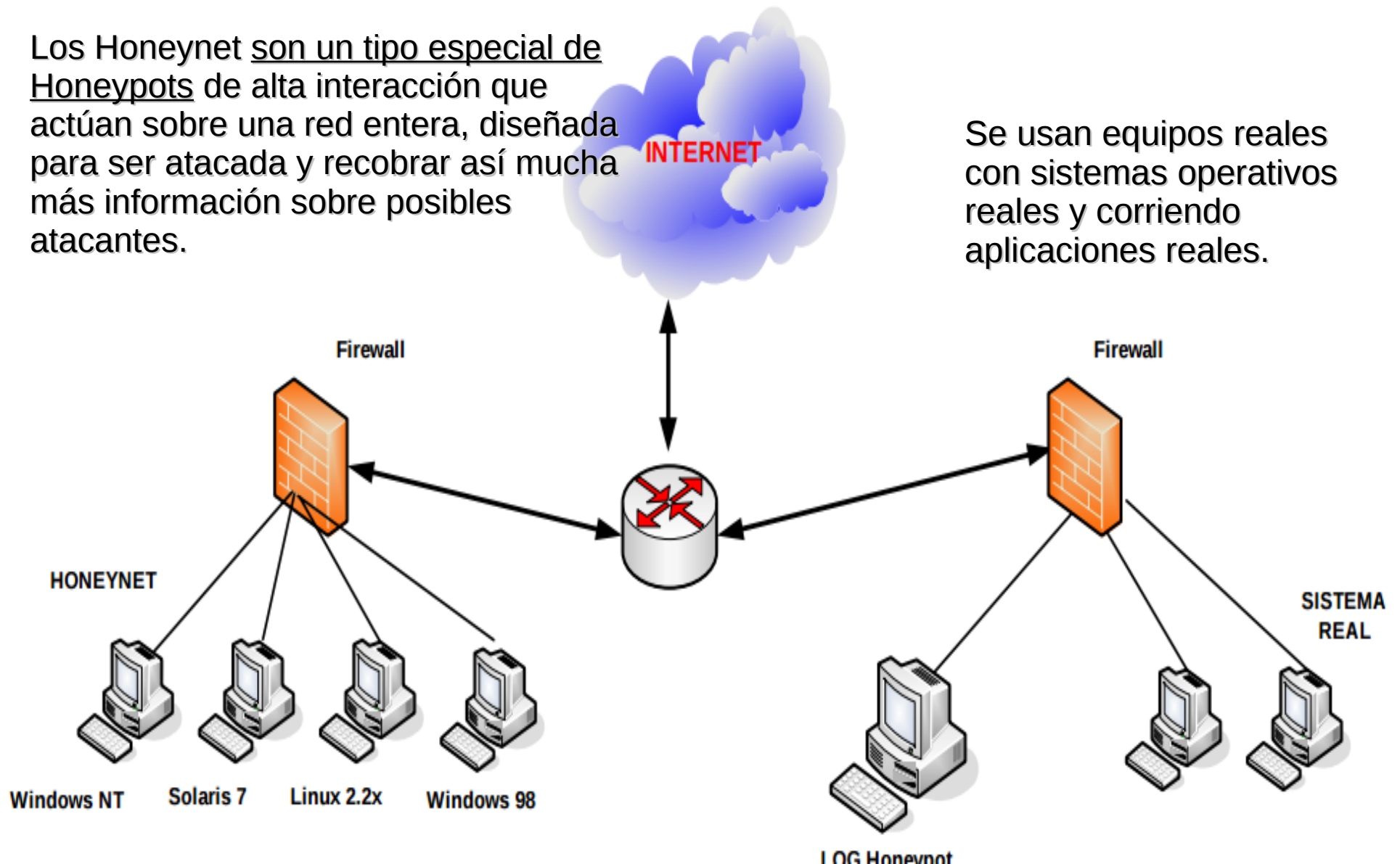
- Zona desmilitarizada



Honeynet

Los Honeynet son un tipo especial de Honeypots de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes.

Se usan equipos reales con sistemas operativos reales y corriendo aplicaciones reales.



VENTAJAS

- Generan pocos datos y de alto valor
- No permite el acceso a ellos
- Se necesitan recursos mínimos
- Sirve tanto para ataques internos, como externos

DESVENTAJAS

- Elementos totalmente pasivos
- Fuentes potenciales de riesgo para nuestra red
- Consumen una dirección IP como mínimo

Como conclusión...

- Los Honeypots tienen un limitado carácter preventivo
- Tienen un alto grado de detección
- La reacción

¿Alguna pregunta ?

