XXIV SALÓN DE INFORMÁTICA

Seguridad Basada en Open Source

La seguridad no depende en ninguna medida de la capacidad de sus dispositivos ni productos.

Mas depende de sus politicas y planes.

Andres Ricardo Almanza Junco
andres.almanza@ubiquando.com.co

“Encontrando el camino hacia el Software Libre”

Objetivos

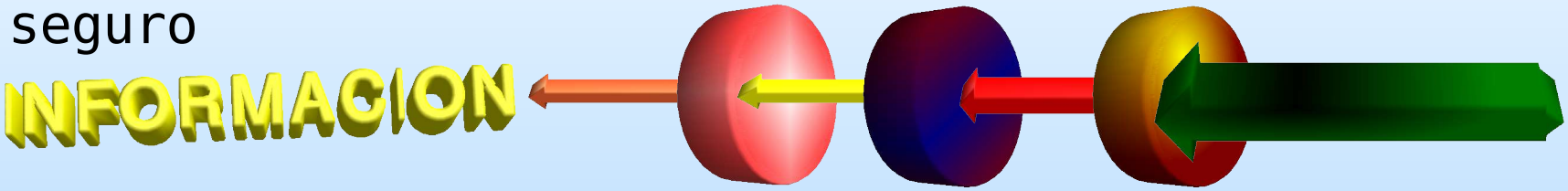
- Mostrar los principales aspectos de la seguridad informática.
- Mostrar las herramientas que existen en software libre para la seguridad informática
- Mostrar por qué es recomendable usar software libre, para la seguridad informática.

Plan de Temas

- Definiciones y Principios de la Seguridad
- Panorama General de la Seguridad
- Por Que Open Source
- Soluciones de seguridad en ambientes Open Source
- Conclusiones

Definiciones y Principios de la Seguridad

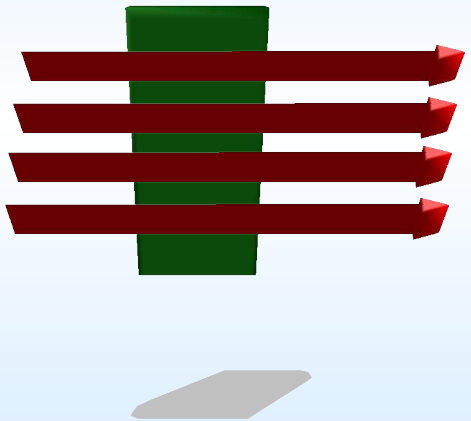
- No es un producto final, es un proceso continuo.
- Mitos no reales (Firewall)
- Crecimiento Continuo de incidentes de Seguridad. Mas de 137,529 hasta la fecha.
- Barreras de protección.
- La seguridad de un sistema involucra: configurar, mantener, y operar un sistema en un ambiente seguro



Definiciones y Principios de la Seguridad

- Cualquier sistema de información debe garantizar los siguientes aspectos o principios:

  - Confidencialidad
  - Integridad
  - Disponibilidad



  - Auntenticacion
  - Autorizacion
  - No Repudio
  - Auditabilidad

Panorama General de la Seguridad

HACKING

Auditoría Informática

Pruebas al plan de Continuidad del Negocio

Implantación Arquitectura

Implantación Plan de Entrenamiento

Implantación Plan continudad del negocio

Clasificación de Información

Diseño Plan de Continuidad del Negocio

Diseño Plan de Entrenamiento del Modelo

Diseño Arquitectura de Seguridad Informática (FW, VPN, IDS, Antivirus, LDAP, PKI, Autenticación Fuerte, CSIRT)

Función de Seguridad Informática

Métricas Area de Seguridad Informática

Modelo de Seguridad Informática (Políticas ISO 17799, Estándares y Procedimientos)OSSTMM (Open Source Security Testing Metodology Manual)

Costo Total de Oportunidad del Modelo

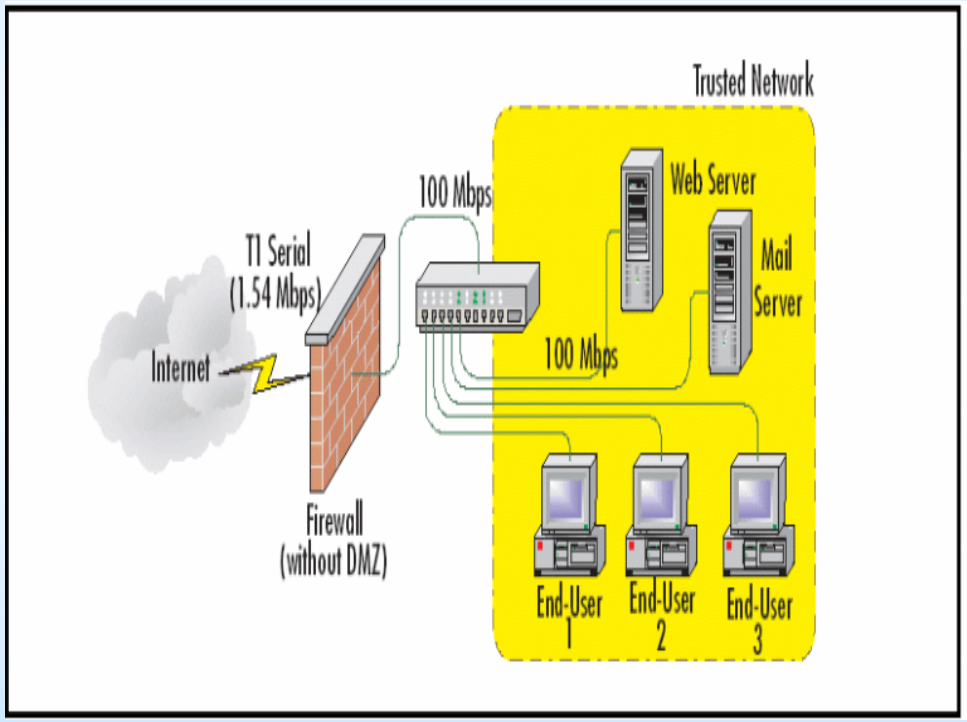
Análisis de Riesgos, Capacity Planning e Impacto en el Negocio

Por que Open Source para la seguridad

- Se conoce que es lo que se ejecuta.
  - Vincent Rijment. Creador de AES. “No solo por que las personas pueden observar lo que se ha escrito, sino por que se forza a la gente ha escribir el codigo de una manera un poco mas clara, para poder adherirse al estandar”.
  - Open Source da el potencia de ser mas seguro que otras plataformas, pero eso no da una garantia total de la seguridad. Elias Levy.

Soluciones de Seguridad en Ambientes Open Source

- Proteccion Perimetral
- Iptables(www.iptables.org)
  - Packet Filter
  - Inspeccion de Paquetes
  - NAT/NAPT
  - Infraestructura flexible
  - Integracion de terceros
  - Repositorio de parches
  - Parte del kernel
  - Administracion

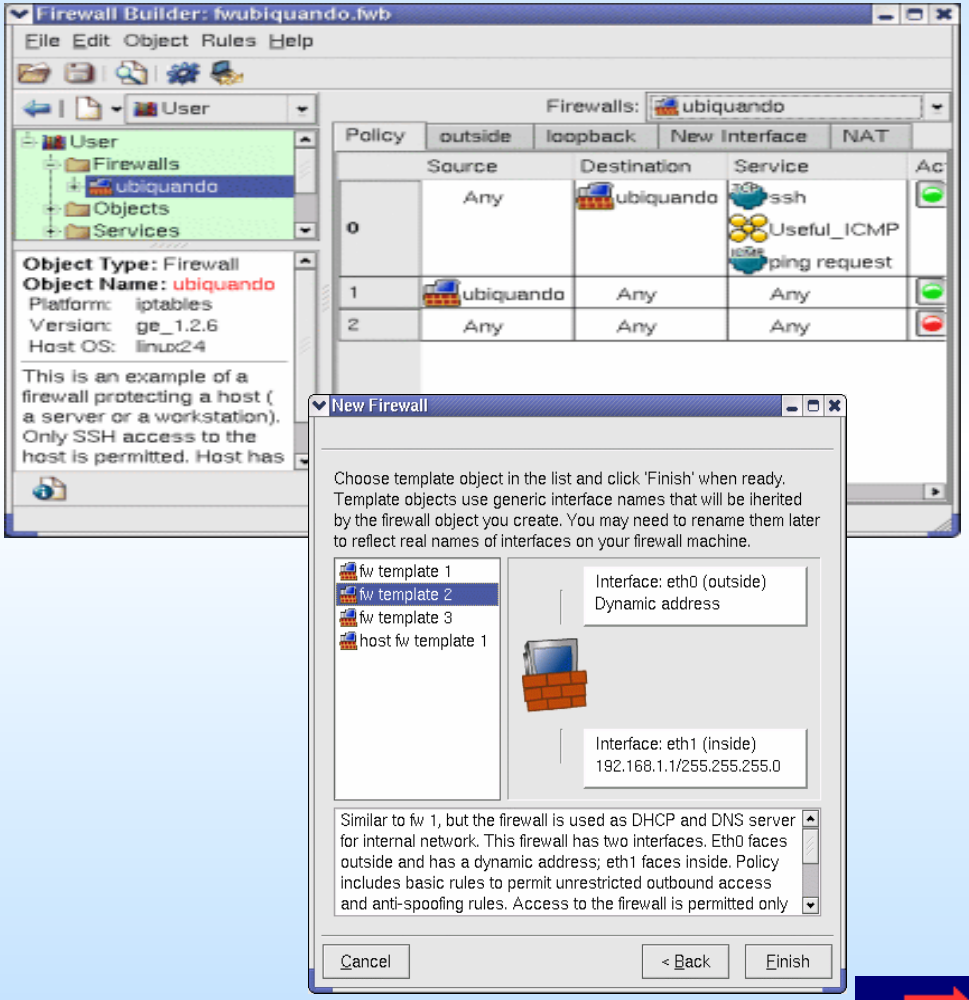


“Encontrando el camino hacia el Software Libre”

Soluciones de Seguridad en Ambientes Open Source

- Herramientas de Adminitracion

- Fwbuilder (www.fwbuilder.org)
- GUI
- Compila politicas para varias plataformas de firewalls. (ipfilter,PF, CIsco,PIX)
- Maneja todo basado en objetos
- Comunicación Remota con la maquina a traves de ssh

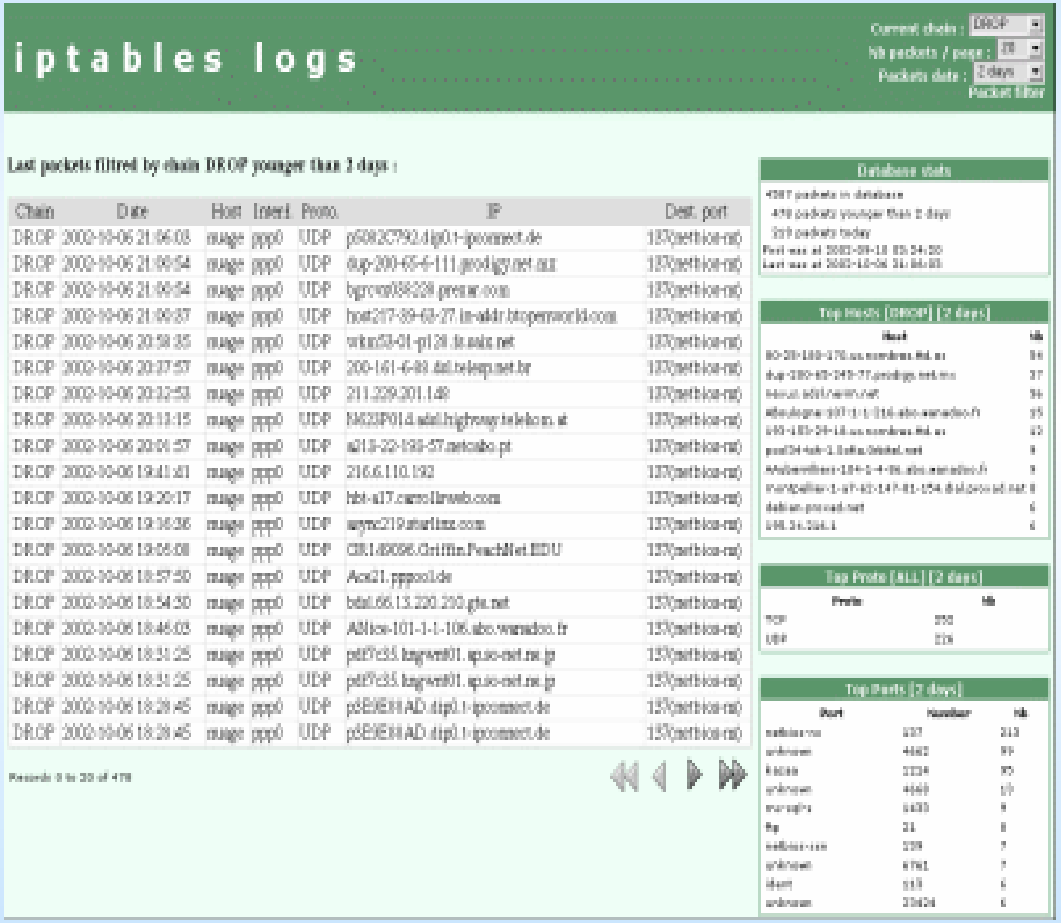


“Encontrando el camino hacia el Software Libre”

Soluciones de Seguridad en Ambientes Open Source

- Herramientas de Adminitracion

- Iptables Log Analizer
- Web-Enable
- Recoleccion de Informacion via demonio
- Almacenamiento en Bases de Datos (Mysql)



“Encontrando el camino hacia el Software Libre”

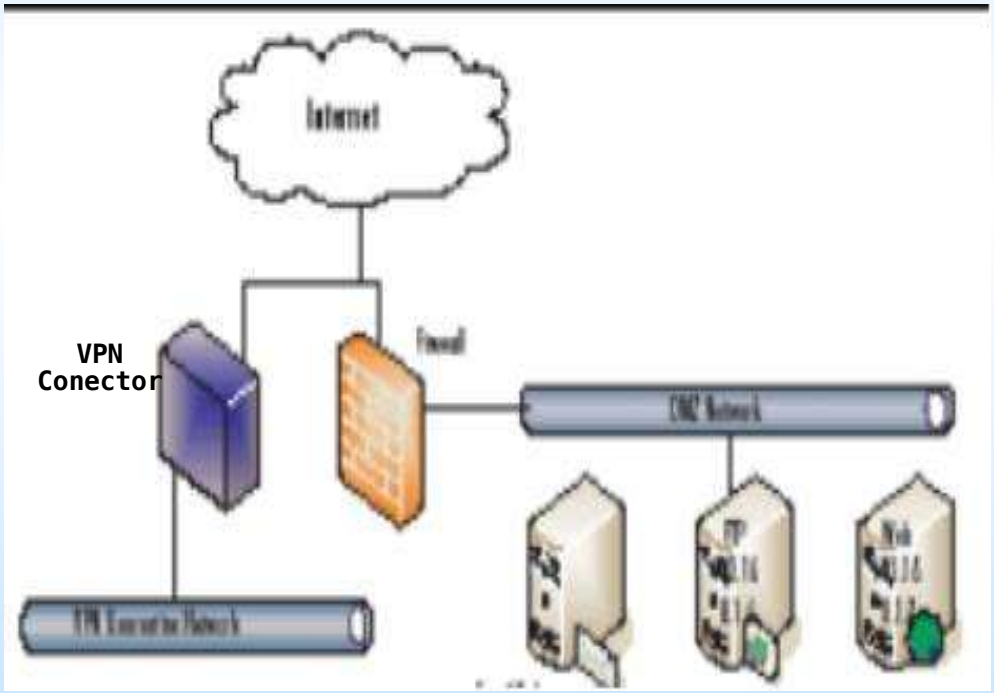
Soluciones de Seguridad en Ambientes Open Source

- Vpns

Openswan

strongSec GmbH
strong internet security

- StrongsWan www.strongswan.org
- Freeswan www.freeswan.org
- OpenSwan www.openswan.org



“Encontrando el camino hacia el Software Libre”

Soluciones de Seguridad en Ambientes Open Source

- Vpns

strongSec GmbH
strong internet security

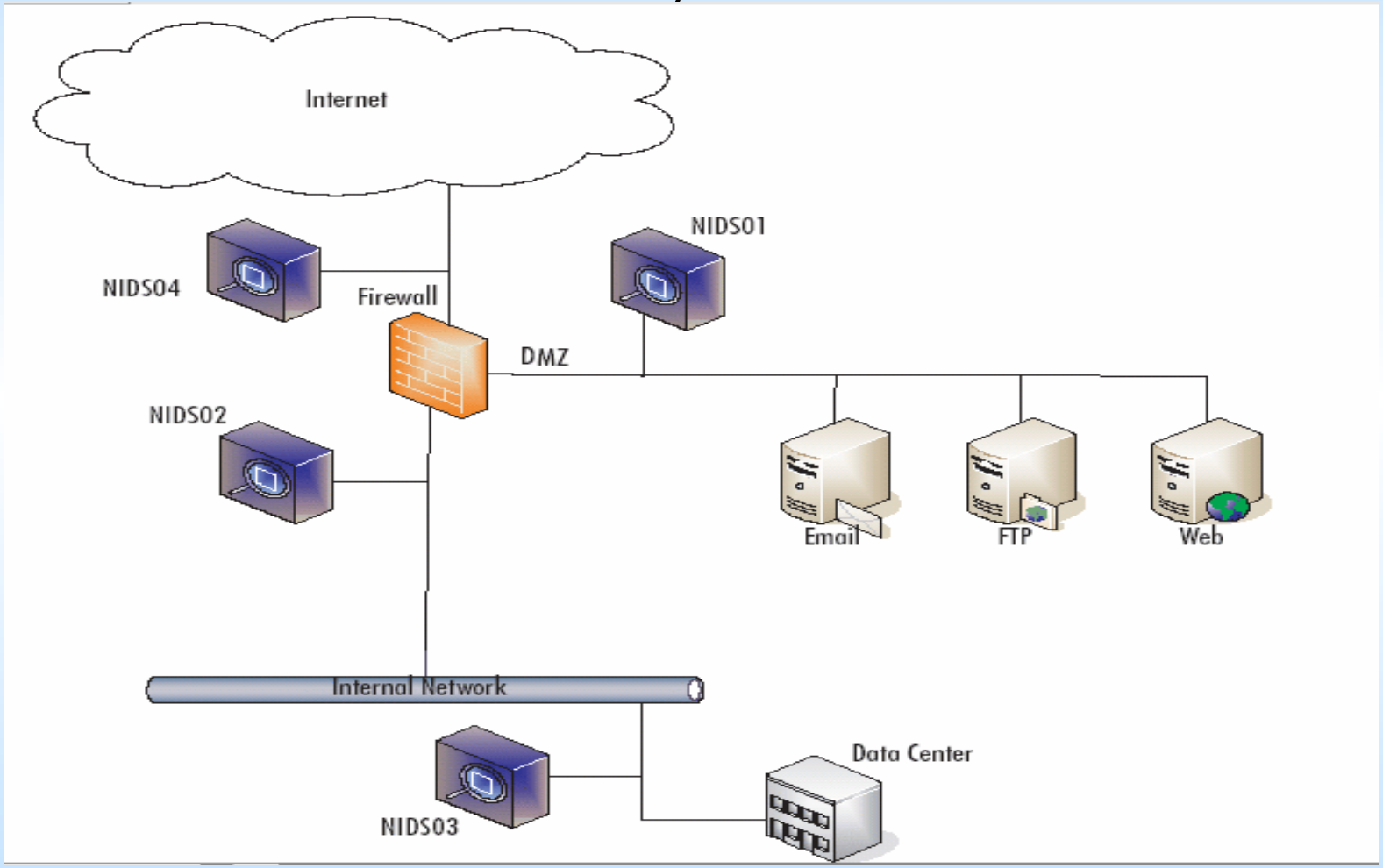
Openswan

- Implementacion de Estandar Ipsec
- Componente adaptable al Kernel
- Integrable con la mayoria de standares IPSec existentes. (VPN-1, entre otros)
- Soporte de Certificados Digitales
- Soporte de Algoritmos de Encripcion
- Evolucion de Fress/Wan en dos nuevos Projectos

“Encontrando el camino hacia el Software Libre”

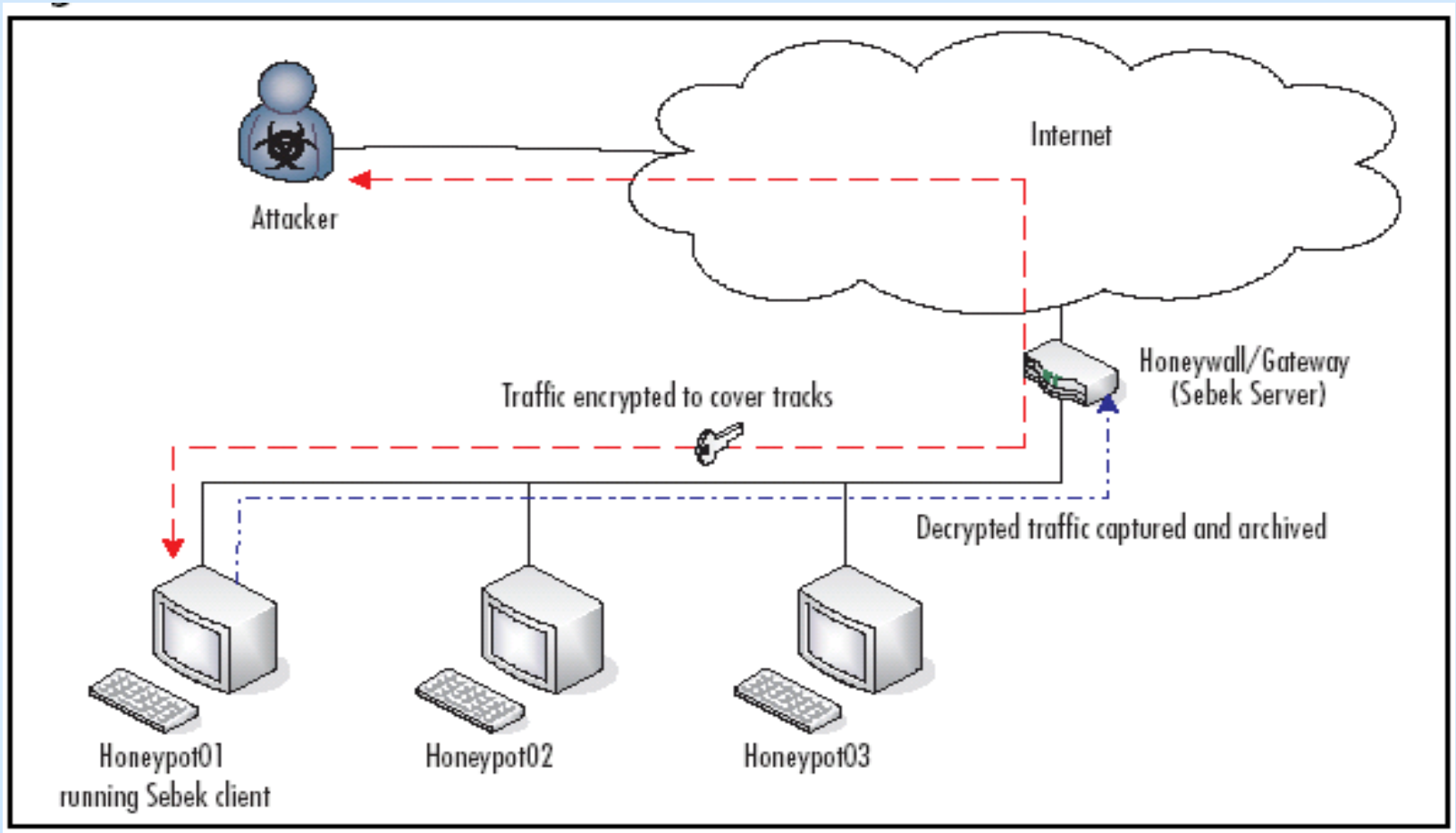
Estructuras de Red

- Proteccion Perimetral y Deteccion de Intrusos

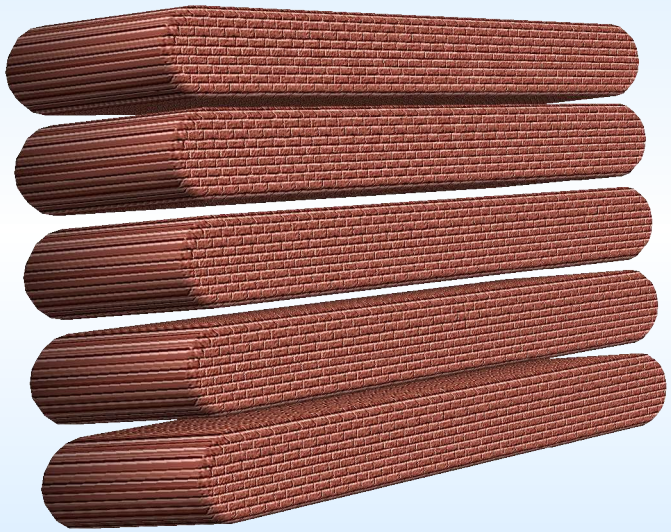


Estructuras de Red

- Sistemas Honeypots



Soluciones de Seguridad en ambientes Open Source



- Proteccion Perimetral

“Encontrando el camino hacia el Software Libre”