



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.

“Encontrando el camino hacia el Software Libre”





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

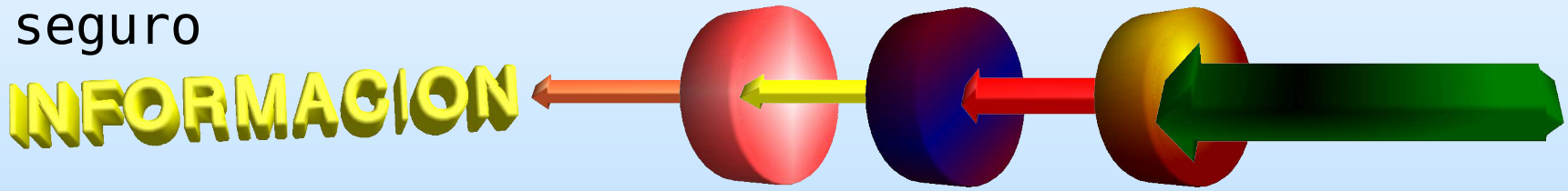
“Encontrando el camino hacia el Software Libre”





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



“Encontrando el camino hacia el Software Libre”





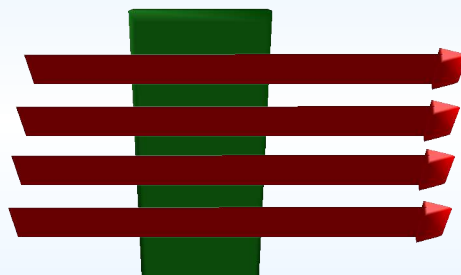
Definiciones y Principios de la Seguridad

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

→ Confidencialidad

→ Integridad

→ Disponibilidad



★ Aunenticacion

★ Autorizacion

★ No Repudio

★ Auditabilidad

“Encontrando el camino hacia el Software Libre”





Panorama General de la Seguridad



“Encontrando el camino hacia el Software Libre”





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.

“Encontrando el camino hacia el Software Libre”



Soluciones de Seguridad en Ambientes Open Source

→ Protección Perimetral

→ Iptables (www.iptables.org)

→ Packet Filter

→ Inspección de Paquetes

→ NAT/NAPT

→ Infraestructura flexible

→ Integración de terceros

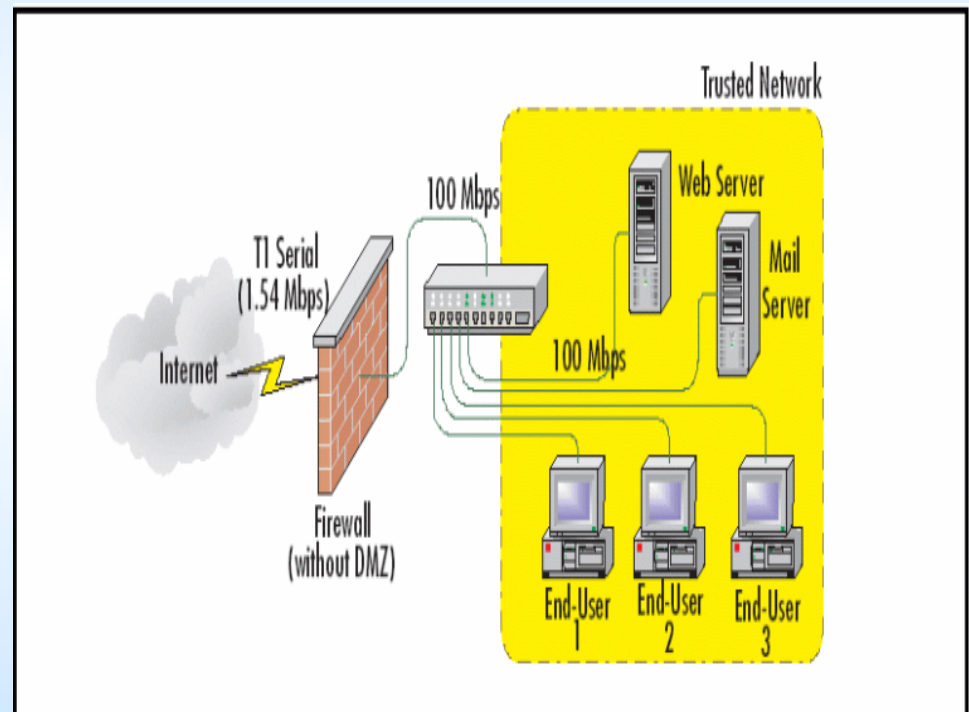
→ Repositorio de parches

→ Parte del kernel

→ Administración

“Encontrando el camino hacia el Software Libre”

netfilter
firewalling, NAT and packet mangling for Linux 2.4



Soluciones de Seguridad en Ambientes Open Source

→ Herramientas de Adminitracion

→ Fwbuilder (www.fwbuilder.org)

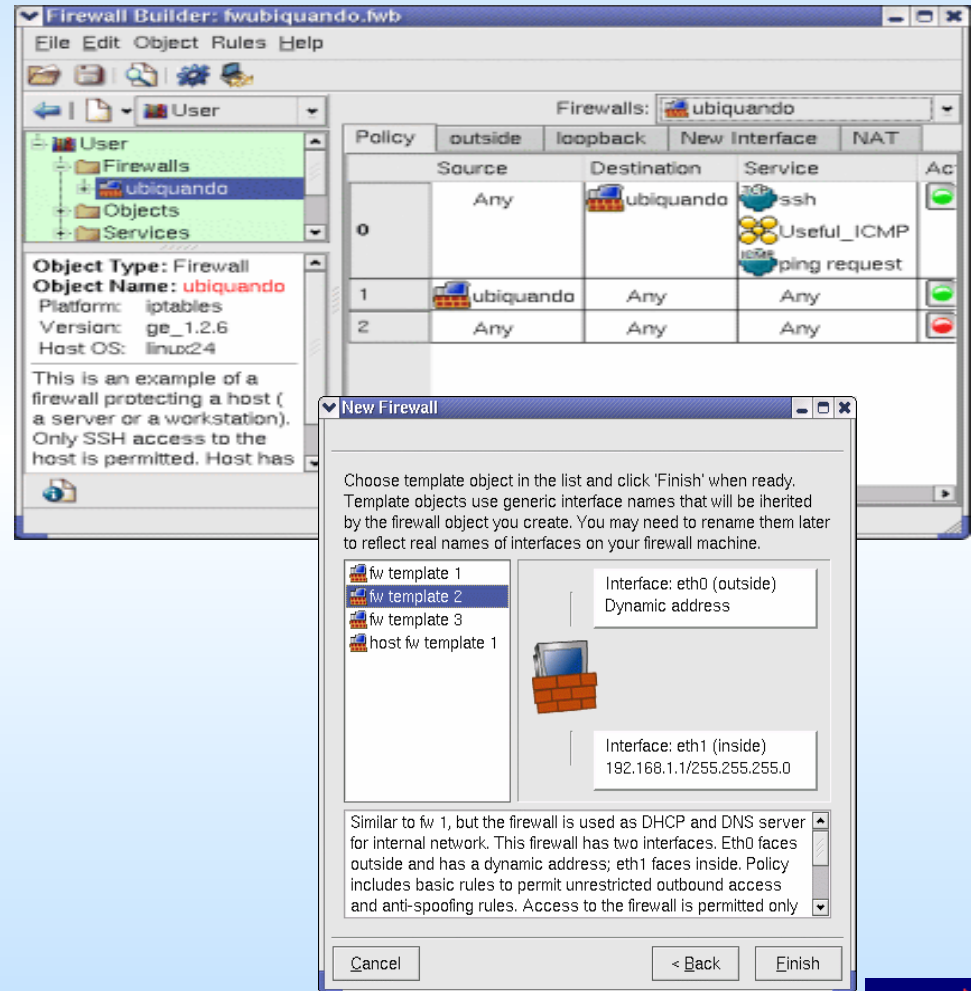
→ GUI

→ 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

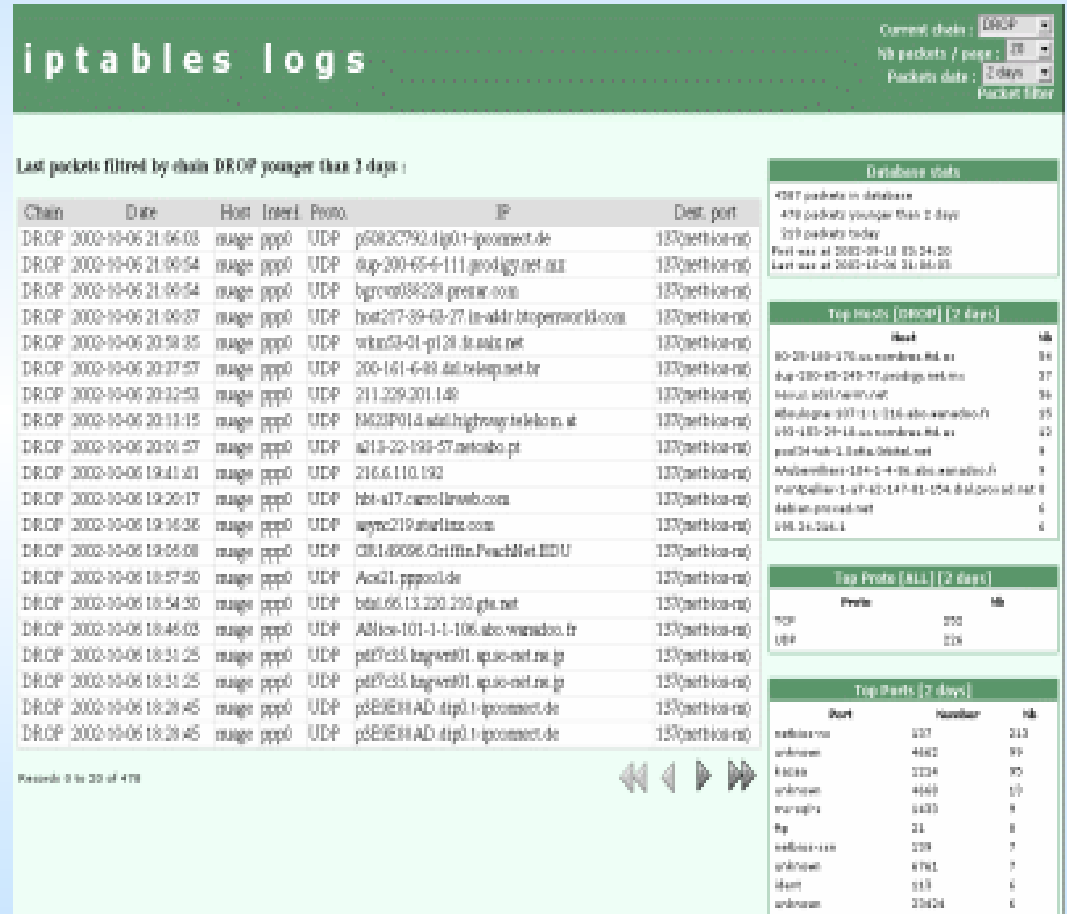
➔ Herramientas de Administracion

➔ Iptables Log Analyzer

➔ Web-Enable

➔ Recoleccion de Informacion via demonio

➔ Almacenamiento en Bases de Datos (Mysql)



The screenshot shows the 'iptables logs' web interface. At the top, there are controls for the current chain (set to 'DROP'), the number of packets per page (set to 20), and the packet date (set to 'today'). Below this, a table displays the last packets filtered by the 'DROP' chain, showing columns for Chain, Date, Host, Inet, Proto, IP, and Dest. port. The table contains 18 rows of log entries. To the right of the main table, there are three summary panels: 'Database stats' showing 4987 packets in the database and 498 packets younger than 2 days; 'Top hosts (today) (2 days)' showing a list of hosts with their counts; and 'Top Ports (ALL) (2 days)' showing a list of ports with their counts. At the bottom of the main table, there are navigation arrows and a page indicator 'Records 0 to 20 of 478'.

Chain	Date	Host	Inet	Proto	IP	Dest. port
DRCP	2003-10-06 21:06:03	muge	ppp0	UDP	p6982C792.dig01-igconnect.de	137(netbios-ns)
DRCP	2003-10-06 21:00:54	muge	ppp0	UDP	dnp-200-69-6-111.godaddy.net.au	137(netbios-ns)
DRCP	2003-10-06 21:00:54	muge	ppp0	UDP	bgprova08208.greiner.com	137(netbios-ns)
DRCP	2003-10-06 21:00:37	muge	ppp0	UDP	hca217-89-60-27.in-addr.btoperworld.com	137(netbios-ns)
DRCP	2003-10-06 20:58:35	muge	ppp0	UDP	wkua03-01-pl28.ds.sds.net	137(netbios-ns)
DRCP	2003-10-06 20:37:57	muge	ppp0	UDP	200-161-6-80.dal.teleport.net.br	137(netbios-ns)
DRCP	2003-10-06 20:32:53	muge	ppp0	UDP	211.209.201.149	137(netbios-ns)
DRCP	2003-10-06 20:13:15	muge	ppp0	UDP	NA23P01.dial.hightway.telecom.at	137(netbios-ns)
DRCP	2003-10-06 20:04:57	muge	ppp0	UDP	a218-20-130-57.netcabo.pt	137(netbios-ns)
DRCP	2003-10-06 19:41:21	muge	ppp0	UDP	216.6.110.192	137(netbios-ns)
DRCP	2003-10-06 19:30:17	muge	ppp0	UDP	hbl-a17.cisco.lirweb.com	137(netbios-ns)
DRCP	2003-10-06 19:16:26	muge	ppp0	UDP	wyrc219.parkerline.com	137(netbios-ns)
DRCP	2003-10-06 19:05:08	muge	ppp0	UDP	CR1-18086.CritFin.PeachNet.EDU	137(netbios-ns)
DRCP	2003-10-06 18:57:50	muge	ppp0	UDP	Acs21.pppool.de	137(netbios-ns)
DRCP	2003-10-06 18:54:30	muge	ppp0	UDP	batal.66.13.200.200.gta.net	137(netbios-ns)
DRCP	2003-10-06 18:46:03	muge	ppp0	UDP	AMice-101-1-1-106.abo.wanadoo.fr	137(netbios-ns)
DRCP	2003-10-06 18:31:25	muge	ppp0	UDP	pd07c35.kugwin01.ap.sco-net.ru.jp	137(netbios-ns)
DRCP	2003-10-06 18:31:25	muge	ppp0	UDP	pd07c35.kugwin01.ap.sco-net.ru.jp	137(netbios-ns)
DRCP	2003-10-06 18:28:45	muge	ppp0	UDP	pdEVENHAD.stp01-igconnect.de	137(netbios-ns)
DRCP	2003-10-06 18:28:45	muge	ppp0	UDP	pdEVENHAD.stp01-igconnect.de	137(netbios-ns)

“Encontrando el camino hacia el Software Libre”

Soluciones de Seguridad en Ambientes Open Source

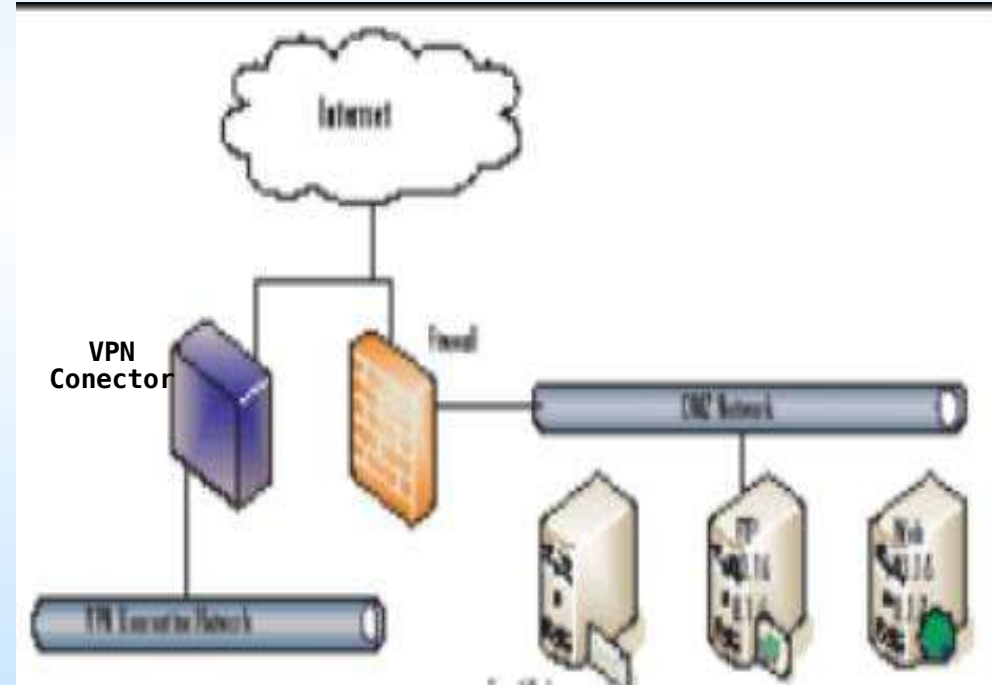


→ Vpns



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



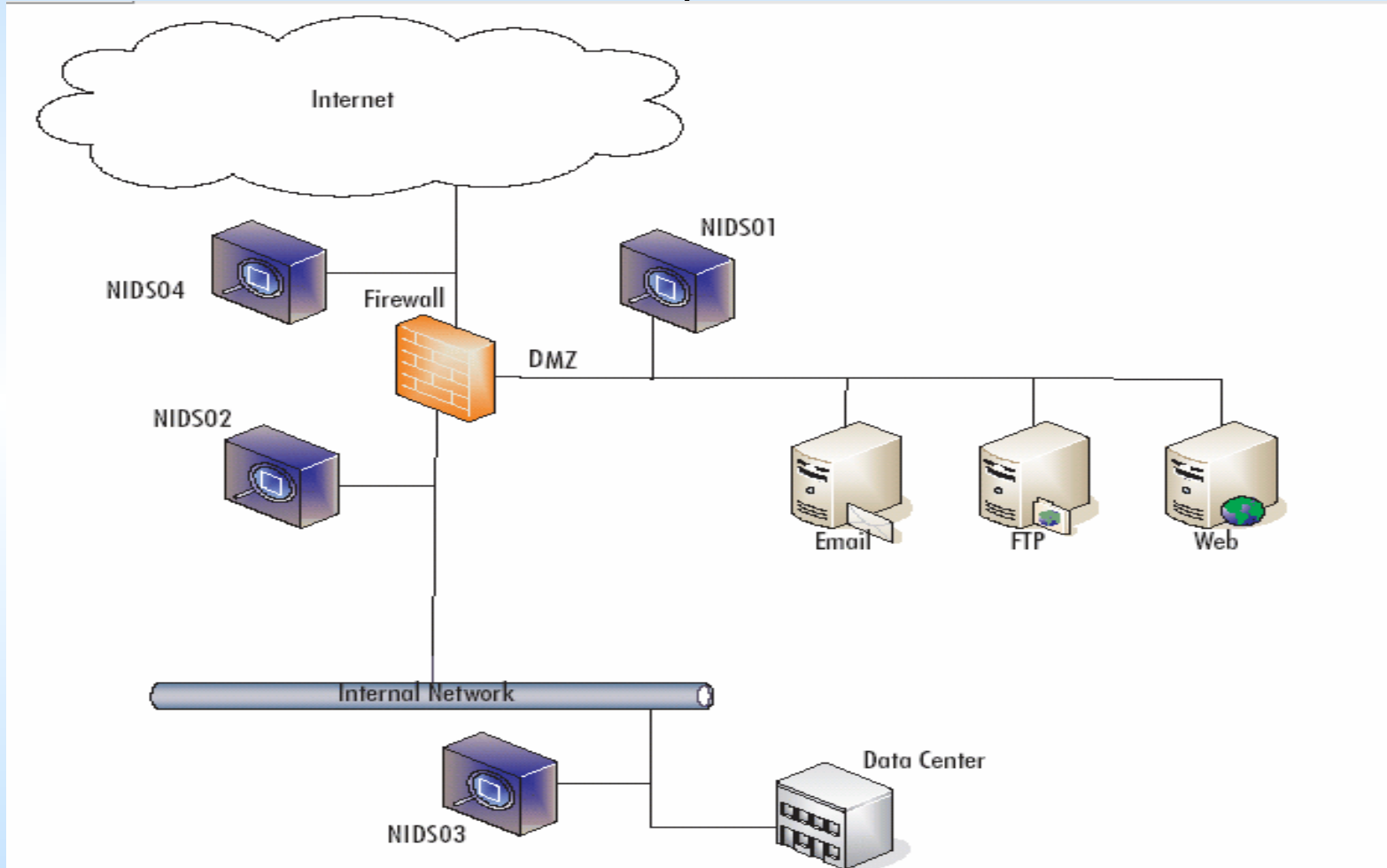
- Implementacion de Estandar Ipsec
- Componente adaptable al Kernel
- Integrable con la mayoria de standares IPsec existentes.
(VPN-1, entre otros)
- Soporte de Certificados Digitales
- Soporte de Algoritmos de Encripcion
- Evolucion de Fress/Wan en dos nuevos Proyectos

“Encontrando el camino hacia el Software Libre”



Estructuras de Red

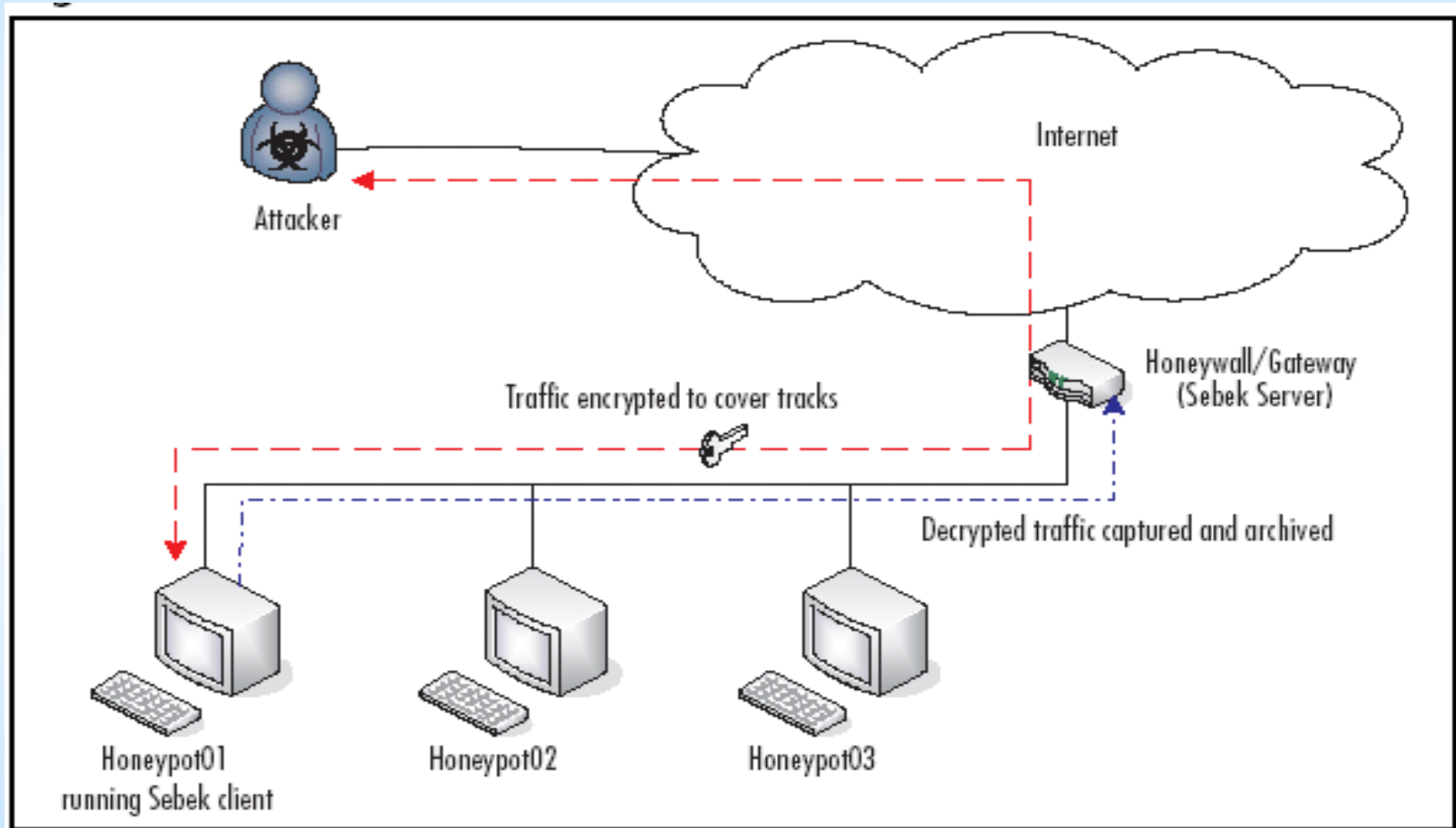
→ Protección Perimetral y Detección de Intrusos



“Encontrando el camino hacia el Software Libre”

Estructuras de Red

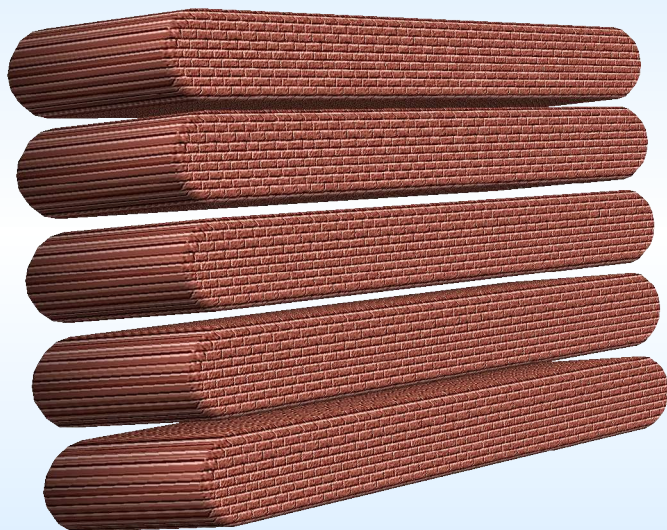
→ Sistemas Honeypots



“Encontrando el camino hacia el Software Libre”



Soluciones de Seguridad en ambientes Open Source



→ Protección Perimetral

“Encontrando el camino hacia el Software Libre”

