

# CORTAFUEGOS PARA REDES INALÁMBRICAS

Dr. Luis Gerardo de la Fraga

Departamento de Computación  
Cinvestav

Correo-e: [fraga@cs.cinvestav.mx](mailto:fraga@cs.cinvestav.mx)

28 de mayo de 2007

Es un cortafuegos dinámico en cual bloquea todo el tráfico hasta que el usuario se registra (o se despliega información de los términos del servicio). La página de inicio intercepta todo el tráfico http, y en su lugar despliega una forma hasta que el usuario es validado. Una vez que se ingresa, todos los puertos, o algunos de ellos, trabajan normalmente.

Por su naturaleza, todas las soluciones de autenticación basadas en portales cautivos son vulnerables al ataque de copia de dirección MAC, y por lo tanto no es una solución invulnerable. Sin embargo, tienen la ventaja de no requerir más software que un navegador de Internet para registrarse en el portal.

Para crear portales captivos para redes inalámbricas, tenemos estas soluciones:

- ▶ NoCAT
- ▶ Wifidog
- ▶ Linux en el mismo punto de acceso

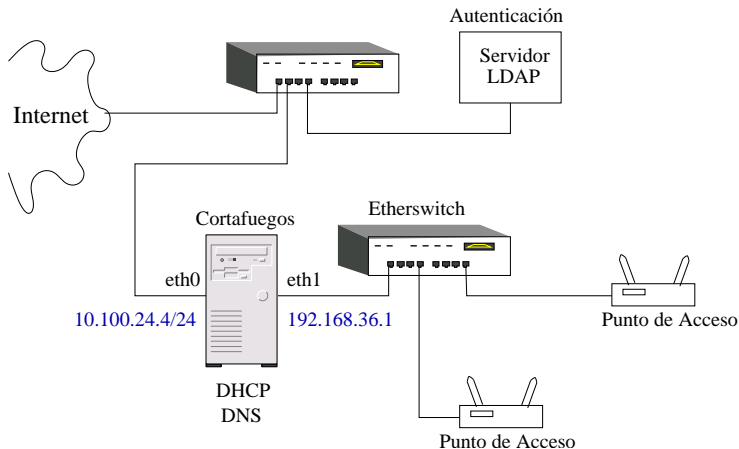
1. NoCAT. Usa PERL. No existe PERL en sistemas empotrados.
2. Wifidog. Escrito en C.
3. Linux en el mismo punto de acceso. Necesitamos comprar el hardware que lo soporta (Linksys).

# CARACTERÍSTICAS DE UNA RED DE PORTALES INALÁMBRICOS

- ▶ Se requiere un cortafuegos con reglas dinámicas. Se usa IPTables.
- ▶ Se requiere un servidor de autenticación.
- ▶ Se requiere un visor del estado de la red de puntos calientes.
- ▶ Se requiere un sistema que administre la red de puntos calientes.

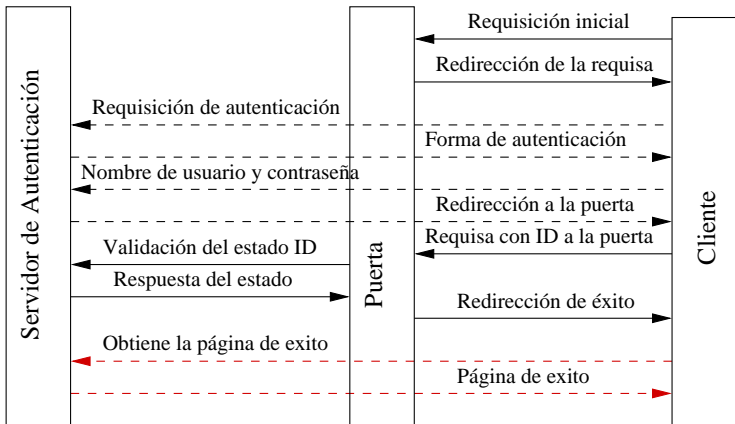
- ▶ LDAP
- ▶ FreeRadius

# SERVIDOR NOCAT PARA LA RED INALÁMBRICA



M. Kershaw, Linux-Powered Wireless Hot Spots, *Linux Journal*, 133, Sep 2003.





El servidor de autenticación en Wifidog realiza lo siguiente:

- ▶ Maneja el registro
- ▶ Monitorea la red en tiempo real
- ▶ Calcula estadísticas sobre patrones de uso de la red y popularidad de los puntos calientes