

Políticas de Seguridad en entornos libres.

Sancho Lerena
slerena@gmail.com



"Software Libre" es cuestión de libertad, no de precio. "Free" en "free software" es una palabra que debe ser traducida como "libre" tal como en "libertad de expresión" ("Free speech"); no como "Gratis" como en "cerveza gratuita" ("Free beer").

www.gnu.org

Índice

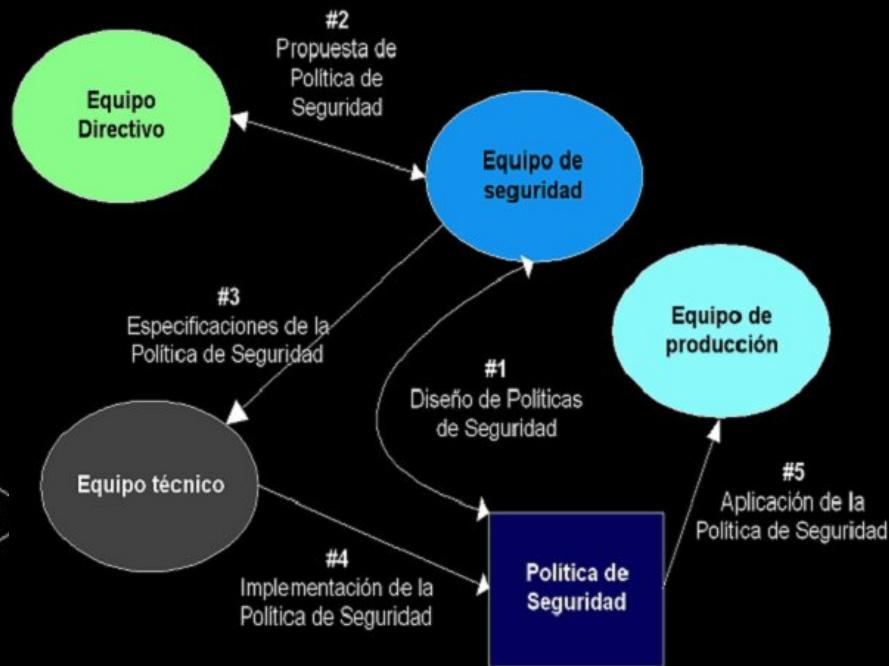
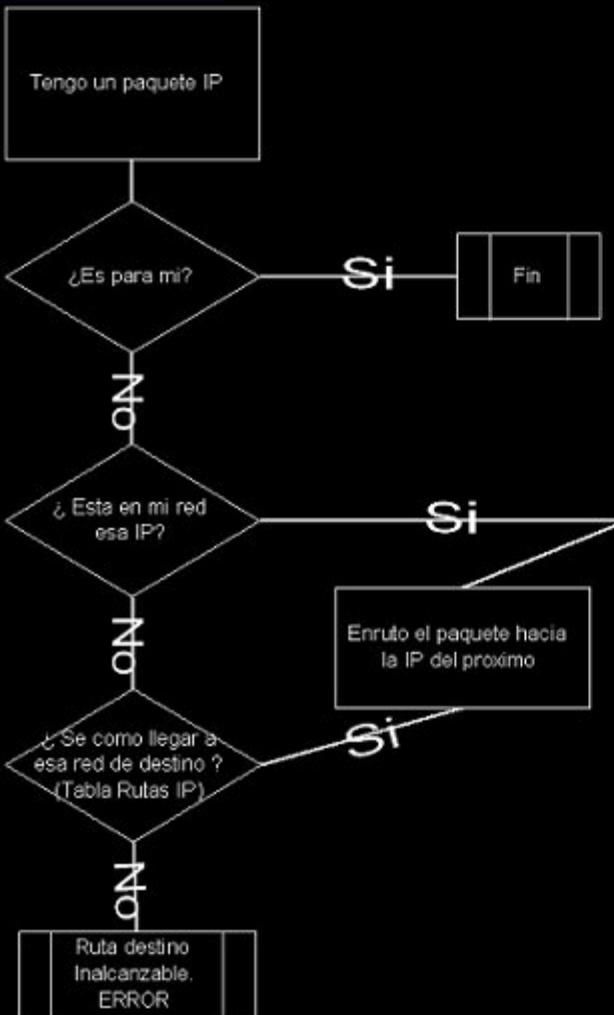
- Parte 1. Introducción
- Parte 2. Políticas de Seguridad
 - ◆ a) Análisis
 - ◆ b) Diseño
- Parte 3. Implementación
 - ◆ a) Arquitectura de redes seguras
 - ◆ B) Seguridad Perimetral
 - ★ 1) Firewall. Netfilter
 - Inspección de estados
 - NAT
 - Filtrado
 - Cadenas
 - Scripting
 - Módulos
 - HA con VRRP

Indice (continuación)

- ◆ B) Seguridad Perimetral (continuación)
 - ★ 2) IDS. Snort
 - Arquitectura
 - Respuestas
 - Integracion de resultados
 - ★ 3) Securización
- ◆ C) QoS. IPRoute2, tc y otros
- ◆ D) Auditoria. Nessus
- ◆ E) Gestión y monitorización
 - ★ MRTG
 - ★ NTP
 - ★ Iptraf
- Parte III. Respuesta ante incidentes.
- Parte IV. Recursos de seguridad.

Avance

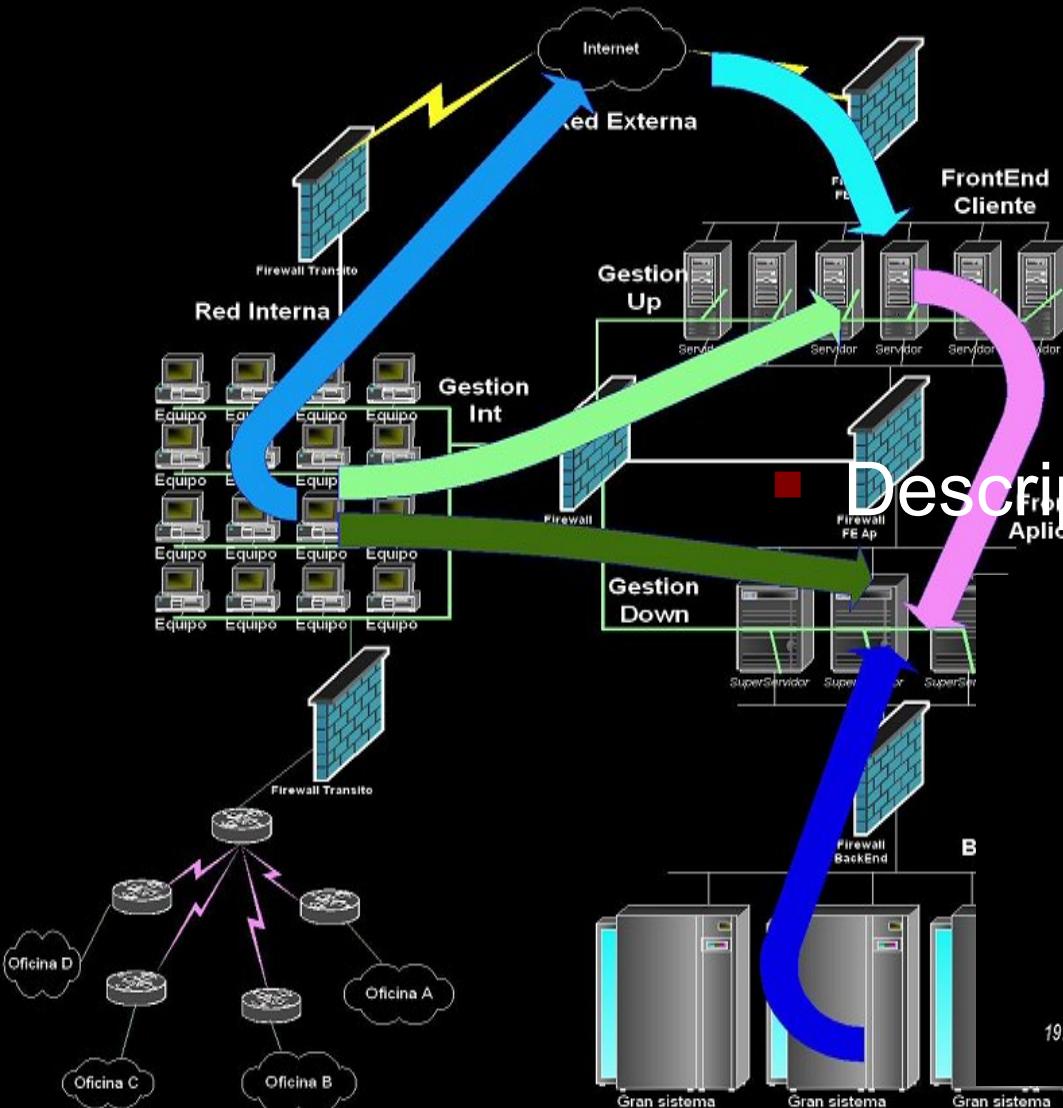
■ Teoría organizativa



■ Funcionamiento Algoritmos

Avance

■ Arquitectura real de redes



■ Descripciones técnicas

#1 Dest -> 212.12.13.2 via 212.12.13.254

#1' 212.12.13.254(Dest) -> 212.12.13.2 via 212.12.13.254

DNAT in ("Manual")

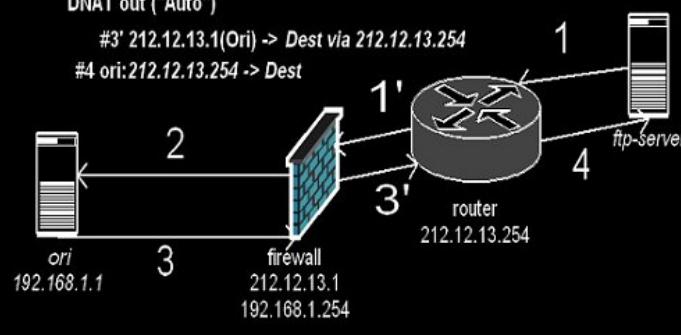
#2 192.168.1.254(Dest) -> 192.168.1.1

#3 ori:192.168.1.1 -> Dest via 192.168.1.254

DNAT out ("Auto")

#3' 212.12.13.1(Ori) -> Dest via 212.12.13.254

#4 ori:212.12.13.254 -> Dest

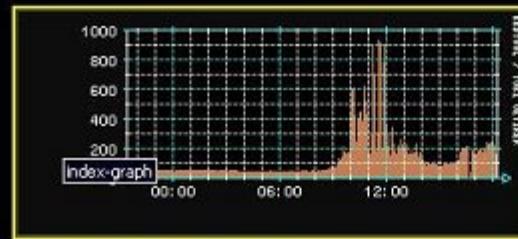


Avance

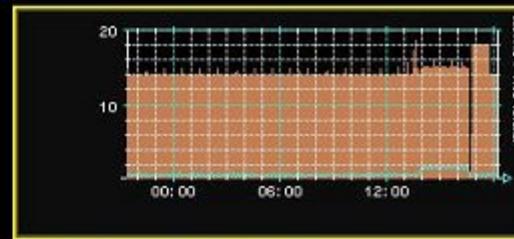
Gestión y control

Total Control
Firewalls
FW-Ext1
FW-Ext2
FW-Ext3
FW-Ext4
FW-ExtGes1
FW-ExtGes2
FW-Int1
FW-Int2
FW-Int3
FW-Int4
FW-IntGes1
FW-IntGes2
Routers
Telia Albacanz
Albacanz->Moraleja
Albacanz->ParcBit
Albacanz->Moraleja
Moraleja->Albacanz
Moraleja->ParcBit
Moraleja->Castellana
ParcBit->Moraleja
ParcBit->Castellana
ParcBit->Moraleja
Castellana->ParcBit
Castellana->Moraleja

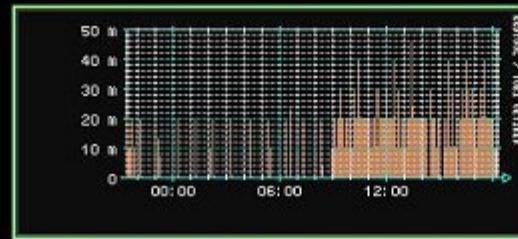
Traffic en FWExt-Gestion1 (Paq/Sec)



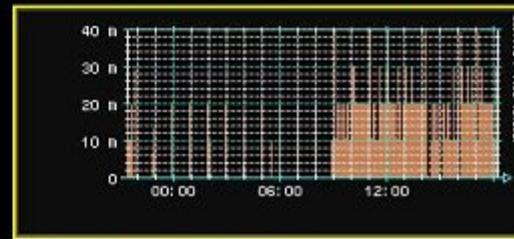
Traffic en FWExt-Gestion2 (Paq/Sec)



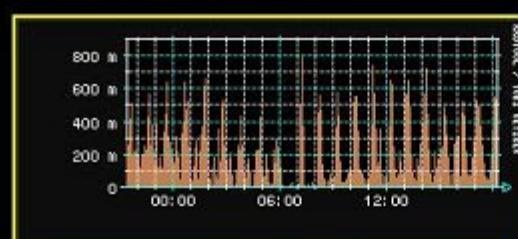
Traffic en FWINT-1 (Paq/Sec)



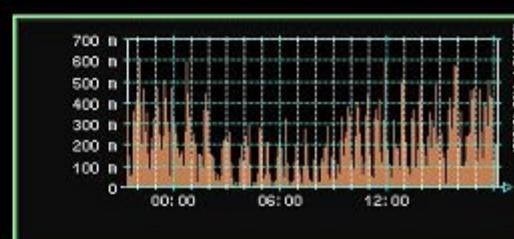
Traffic en FWINT-2 (Paq/Sec)



Traffic en FWINT-3 (Paq/Sec)



Traffic en FWINT-4 (Paq/Sec)



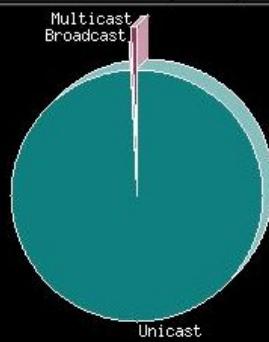
About Data Rcvd Data Sent Stats IP Traffic IP Protos Admin



▶ Stats
Multicast
Traffic
Hosts
Network Load

Global Traffic Statistics

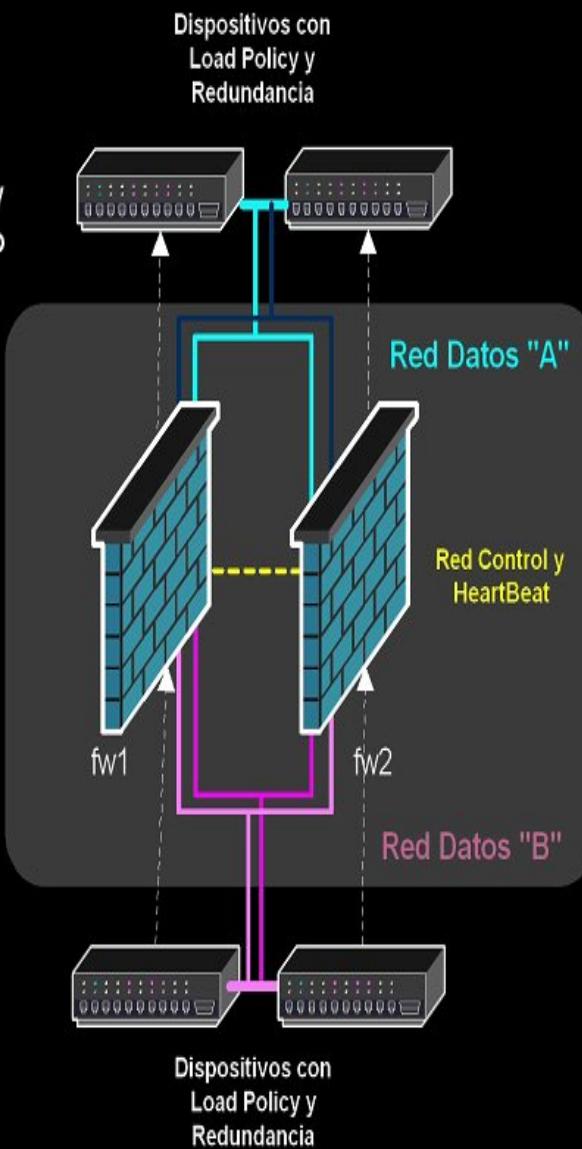
Nw Interface Type	eth1 (Ethernet) [0.0.0.0/255.255.255.255]
Sampling Since	Mon Mar 11 13:29:03 2002 [1 day(s) 5:49:56]
Total	23,454,885
Dropped by the kernel	0
Dropped by ntop	0
Unicast	99.1% 23,243,902
Broadcast	0.0% 703
Multicast	0.9% 210,260



Shortest	60 bytes
Average Size	596 bytes
Longest	1,514 bytes
< 64 bytes	44.5% 10,429,081
< 128 bytes	16.2% 3,804,516
< 256 bytes	9.4% 2,207,388
< 512 bytes	5.7% 1,325,668

Avance

■ Teoría



Firewall HA
Hot-StandBy
con Balanceo

Dispositivos con
Load Policy y
Redundancia

■ ... y práctica

```
#!/bin/bash
# Checking connectivity with ICMP Ping, VRRPD Companion Script
VER="11/03/2002 - v1.0"
SLEEP_TIME=$2                      # Tiempo de parada entre checks, en segundos
if [ -z $2 ]
then
    SLEEP_TIME=5                  # Si no se especifica, el check es cada 5 segundos
fi;
# Obtener el PID de los procesos de VRRPD en memoria
LISTA_PROCESOS=`ps -A | grep "vrrpd" | tr -s " " | cut -d " " -f 2` 
if [ -z "$LISTA_PROCESOS" ]
then
    echo " No VRRP Daemon running, aborting. "
    exit
fi;
IP_DESTINO=$1                      # IP de comprobacion, pasada como 1# parametro
COMANDO=`ping -c 1 "$IP_DESTINO" | grep '100% packet loss'` 
RES=0
while [ "$RES" -eq 0 ];do
    if [ ! -z "$COMANDO" ] ;then
        echo " Ping fail "
        echo " Shutting down VRRP daemons "
        kill -s 9 $LISTA_PROCESOS
        RES=1;else
        echo " Debug: Ping ok"
        sleep $SLEEP_TIME
    fi;done;
```

Parte I. Introducción a la seguridad



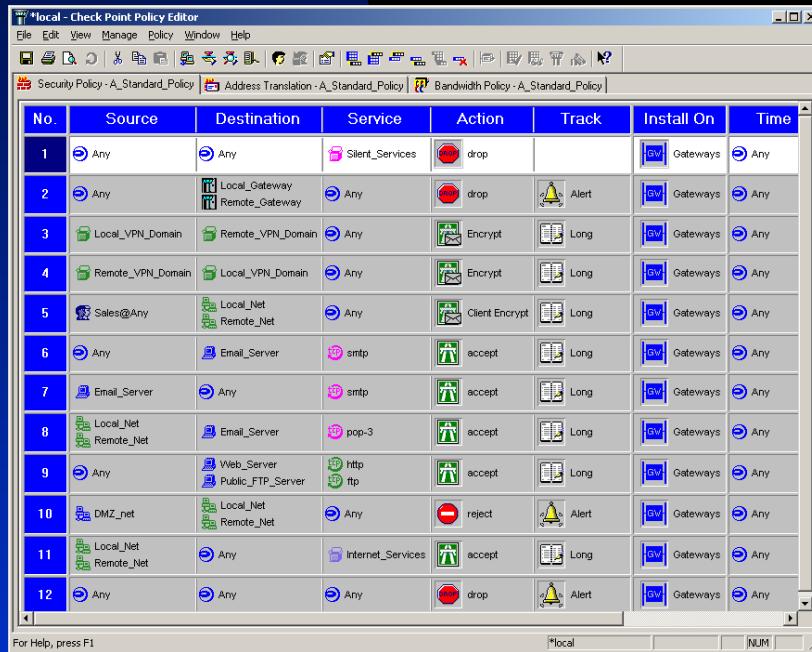
GNU y Seguridad

- ¿ Que es la Seguridad ?.
 - ◆ Logica
 - ◆ Fisica
 - ◆ Redes
 - ★ Firewalls
 - ★ IDS
 - ◆ Hosts
- Software Abierto vs Software Cerrado
 - ◆ Soporte y otros “problemas”



GNU y Seguridad I

■ Software Abierto vs Software Cerrado



```
# Filtrado: FORWARDING
# =====
echo "Activamos filtrado de forward (FORWARD)..."
echo "Dejamos pasar las conexiones ESTABLECIDAS o RELATIVAS a las establecidas..."
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

echo "Las conexiones bidireccionales..."
iptables -A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT          # ping
iptables -A FORWARD -p icmp --icmp-type echo-request -j ACCEPT        # ping
iptables -A FORWARD -p udp --dport 53 -j ACCEPT                         # DNS
iptables -A FORWARD -p udp --sport 53 -j ACCEPT                          # DNS
iptables -A FORWARD -s $LOCALNET -p udp --dport 161:162 -j ACCEPT       # SNMP

echo "Las conexiones entrantes hacia " $IRIS
iptables -A FORWARD -d $IRIS -p tcp --dport 21 -j ACCEPT                # FTP en ARES
iptables -A FORWARD -d $IRIS -p tcp --dport 22 -j ACCEPT                  # SSH
iptables -A FORWARD -d $IRIS -p tcp --dport 23 -j ACCEPT                  # Telnet
iptables -A FORWARD -d $IRIS -p tcp --dport 80 -j ACCEPT                  # HTTP Apache puerto 80
#iptables -A FORWARD -d $IRIS -p tcp --dport 8080 -j ACCEPT               # HTTP Proxy SQUID
iptables -A FORWARD -d $IRIS -p tcp --dport 25 -j ACCEPT                  # SMTP
iptables -A FORWARD -d $IRIS -p tcp --dport 110 -j ACCEPT                 # POP
iptables -A FORWARD -d $IRIS -p tcp --dport 443 -j ACCEPT                  # HTTPS
iptables -A FORWARD -d $IRIS -p tcp --dport 6346 -j ACCEPT                 # Gnutella

echo "Las conexiones entrantes hacia " $HERCULES
iptables -A FORWARD -d $HERCULES -p tcp --dport 261 -j ACCEPT             # Pruebas CURRO ***** (Auth FW-1)
iptables -A FORWARD -d $HERCULES -p tcp --dport 5900 -j ACCEPT              # VNC
iptables -A FORWARD -d $HERCULES -p tcp --dport 21 -j ACCEPT                  # FTP en Hercules
iptables -A FORWARD -d $HERCULES -p tcp --dport 4661 -j ACCEPT                 # eDonkey2000
iptables -A FORWARD -d $HERCULES -p tcp --dport 5631 -j ACCEPT                  # PCAnywhere

echo "Las conexiones entrantes hacia " $ARES
iptables -A FORWARD -d $ARES -p tcp --dport 5901 -j ACCEPT # VNC
iptables -A FORWARD -d $ARES -p tcp --dport 23 -j ACCEPT # SSH
```

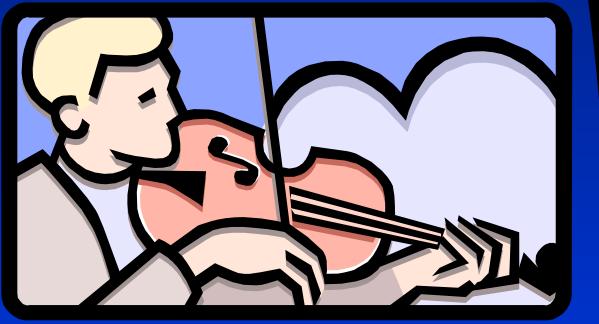
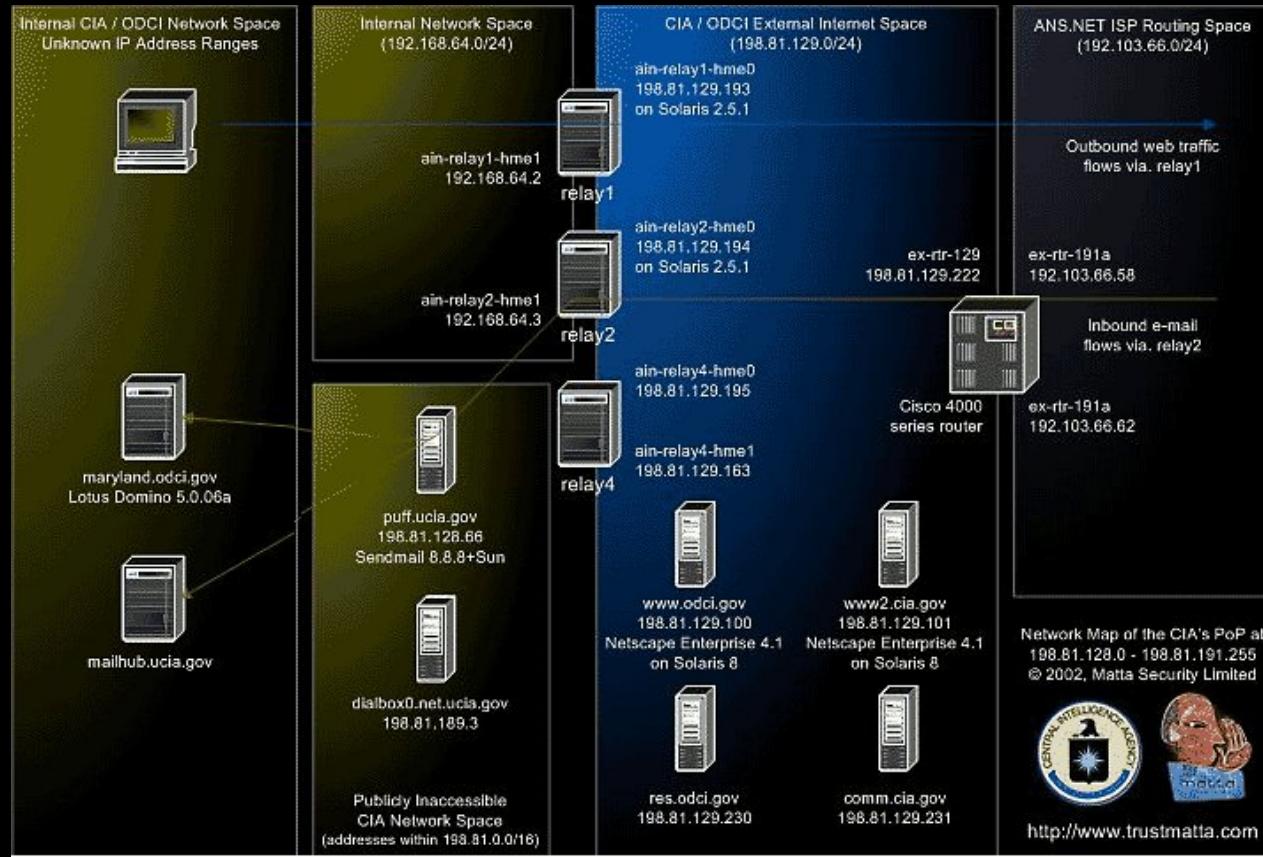
GNU y Seguridad II

- GNU y Empresa
- Teoría vs Practica
 - ◆ Falta de conocimientos
 - ◆ Prisas y falta de profesionalidad
 - ◆ GUI's
- ¿ Es GNU Seguro ?
 - ◆ Código Abierto
 - ◆ Documentación



Un poco de miedo I

- Un buen día....



Un poco de miedo II

■ Algunos sucesos curiosos (13/3/02)



A screenshot of a Mozilla browser window showing the Slashdot homepage. The title bar reads "Slashdot: News for nerds, stuff that matters - Mozilla {Build ID: 2002031104}". The address bar shows "http://snort.org". A search bar is present. The main content area features a banner with the text "Want to see your name on" and a logo. A modal dialog box titled "Alert" displays the message "www.snort.org could not be found. Please check the name and try again." with an "OK" button. The background of the page includes a navigation menu on the left and a sidebar with news links on the right.

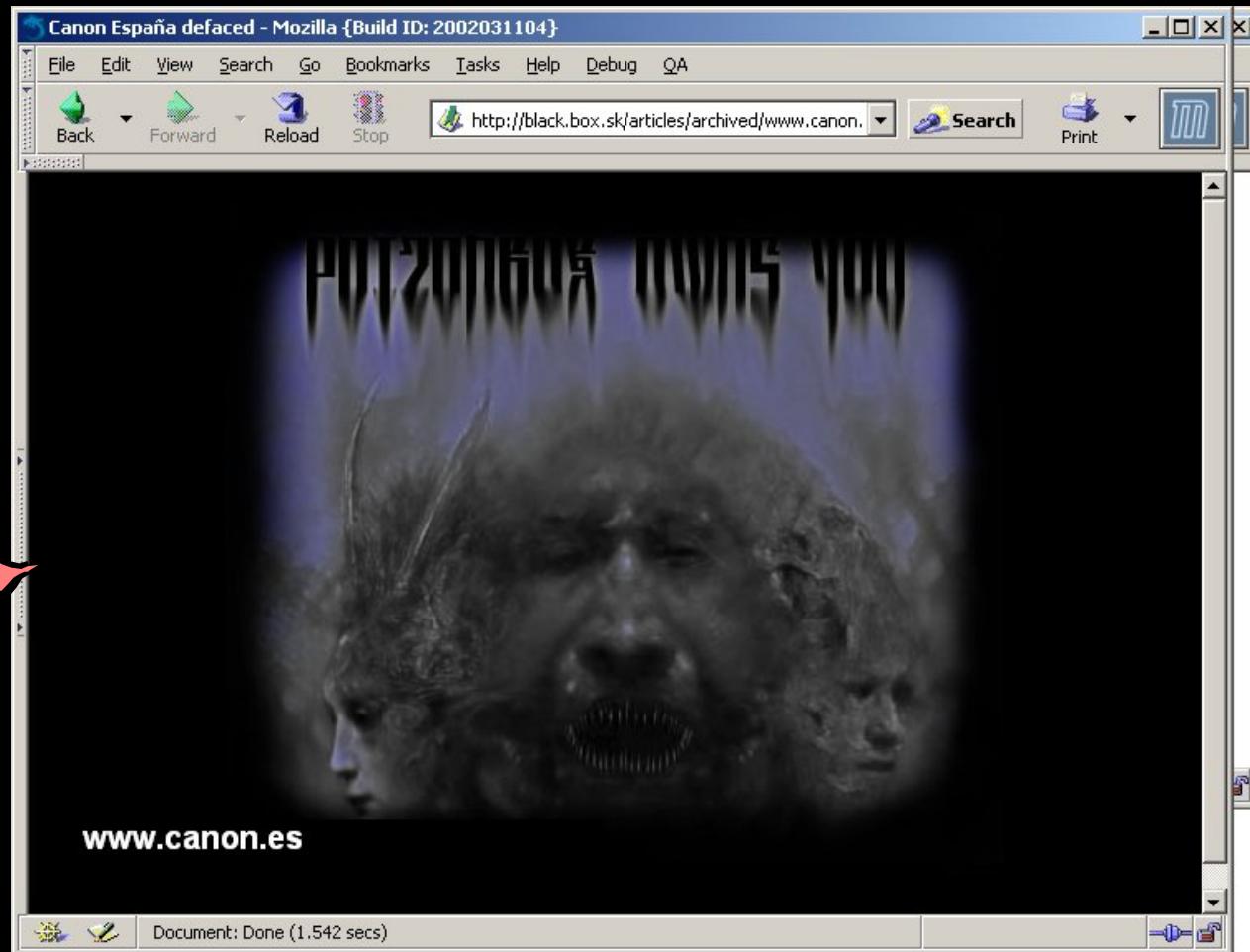
Un poco de miedo III

- www.securitybase.com



Un poco de miedo IV

- [www.canon.es](http://black.box.sk/articles/archived/www.canon.es)



Un poco de miedo V

- www.securecreditcard.net



MNS MNS MNS - Mozilla {Build ID: 2002031104}

File Edit View Search Go Bookmarks Tasks Help Debug QA

Back Forward Reload Stop http://black.b... Search Print

Stop loading this page

```
Connected to target.  
Escape character is '^]'.  
  
-----  
| owned by: Tw34k  
| mnssecure@hotmail.com  
|  
| greetz: sENsE - Xentric - D-force - data cha0s  
| world-of-hell - Prime suspectz - null  
|-----  
  
[root@mns_ownz_you root]#
```

Document: Done (0.631 secs)

Un poco de miedo VI

- www.exodus.it

Violated by GraNde_MuLo - Mozilla {Build ID: 2002031104}

File Edit View Search Go Bookmarks Tasks Help Debug QA

Back Forward Reload Stop http://black.box.sk/art Search Print



WANTED
GraNde MuLo
\$1,000,000
DEAD OR ALIVE

Begin....

Purtroppo non posso fare molto per voi..
la vostra attivita' e' molto importante.

Dedicato a: Samba Diouf,
perche' nessuno merita di morire come e' morto lui.
forse solo i suoi assasini. Forse.

EOF.

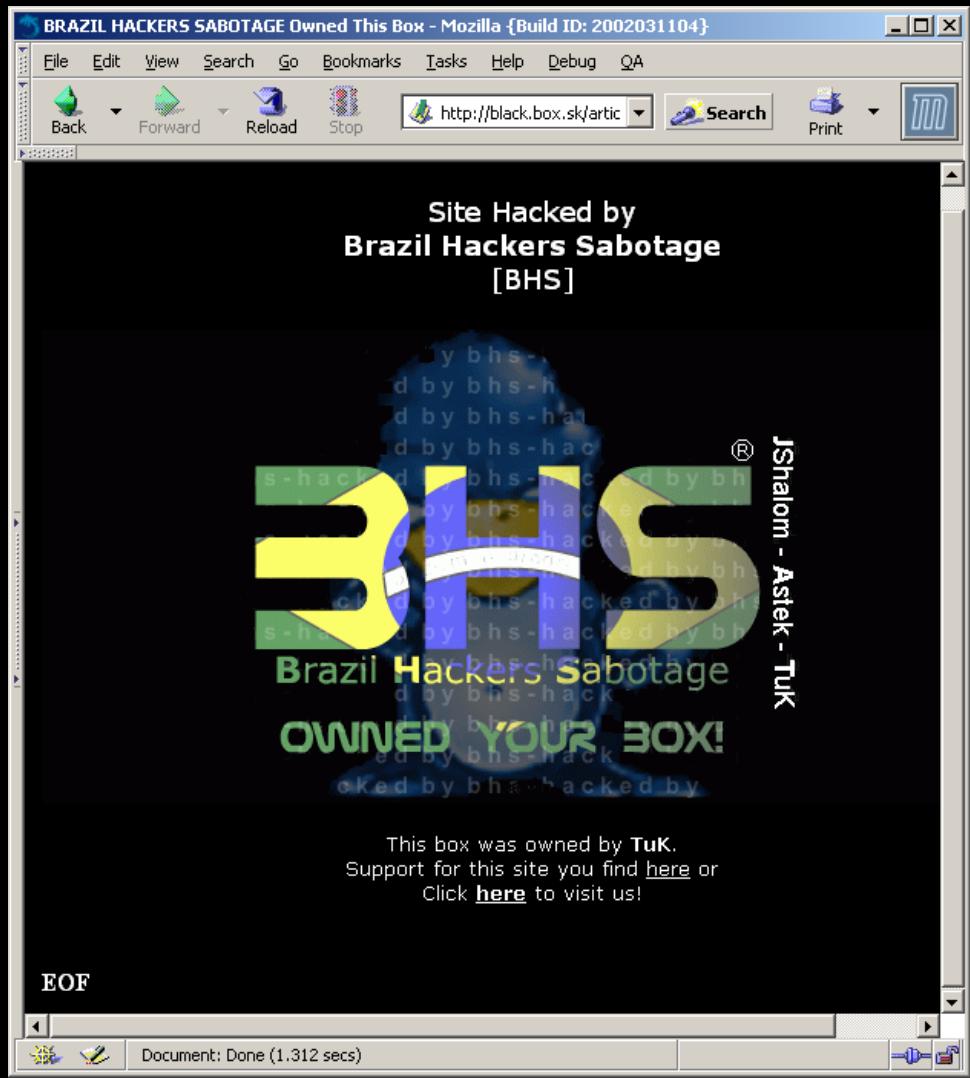
GraNde_MuLo

Document: Done (1.022 secs)



Un poco de miedo VII

■ www.comntel.com



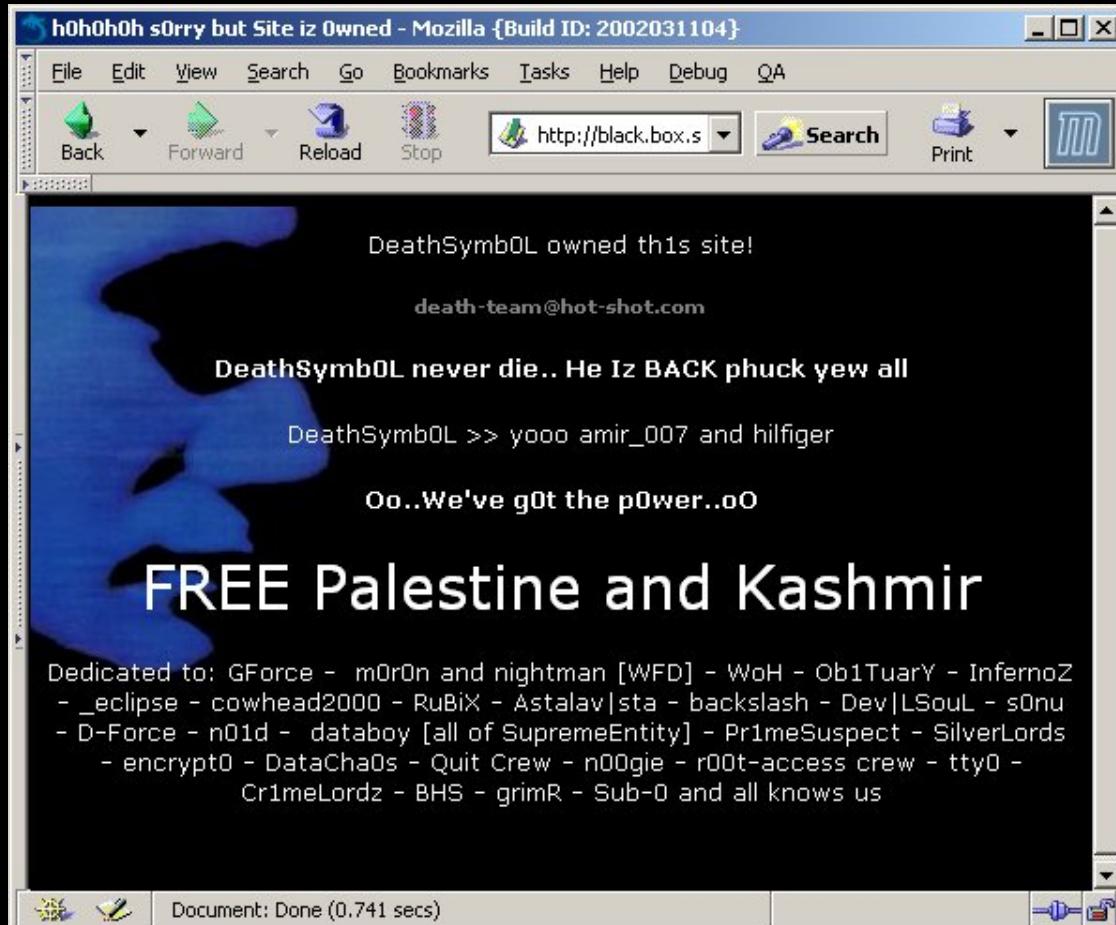
Un poco de miedo VIII

■ www.fox.dk



Un poco de miedo IX

■ www.kenwood.cd



Un poco de miedo X

- Algunas noticias sobre seguridad

(neworder.box.sk)

IT security pros learn to beat hackers at their own game

@ SMS Mar 14 2002 - 01:26 EST

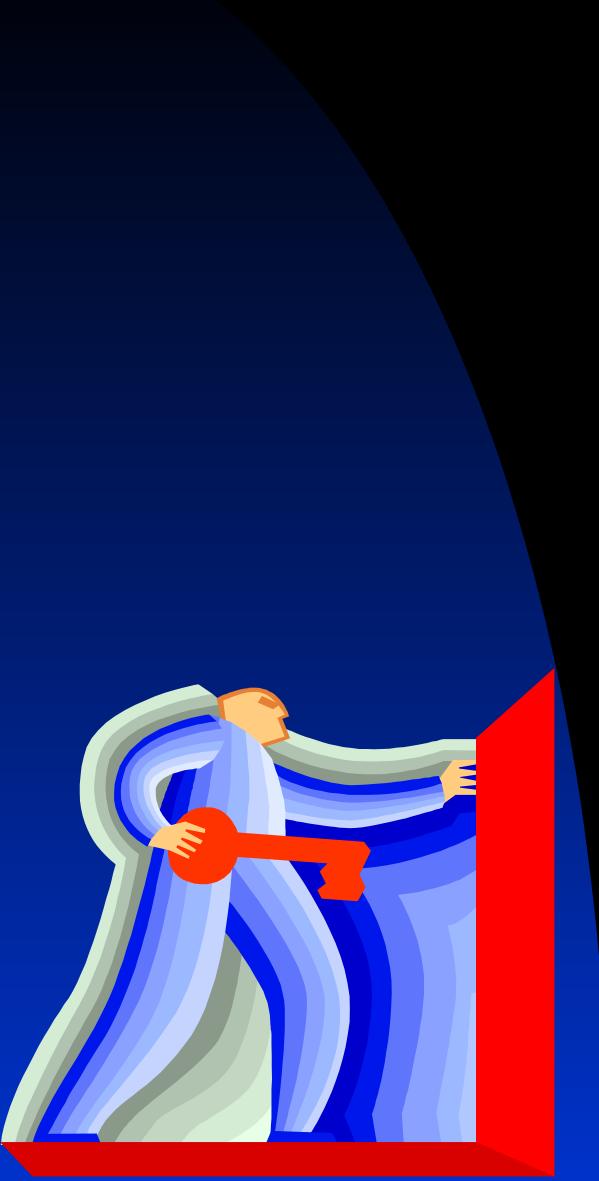
The **_MadMan** writes: Corporate security and IT professionals got a chance last week to think like hackers so they could learn how to better prevent unauthorized users from gaining access to their networks.

More than a dozen computer specialists from across the country took part in an intensive five-day "boot camp" offered by New York-based Ernst & Young LLP on the defense of enterprise networks. They paid

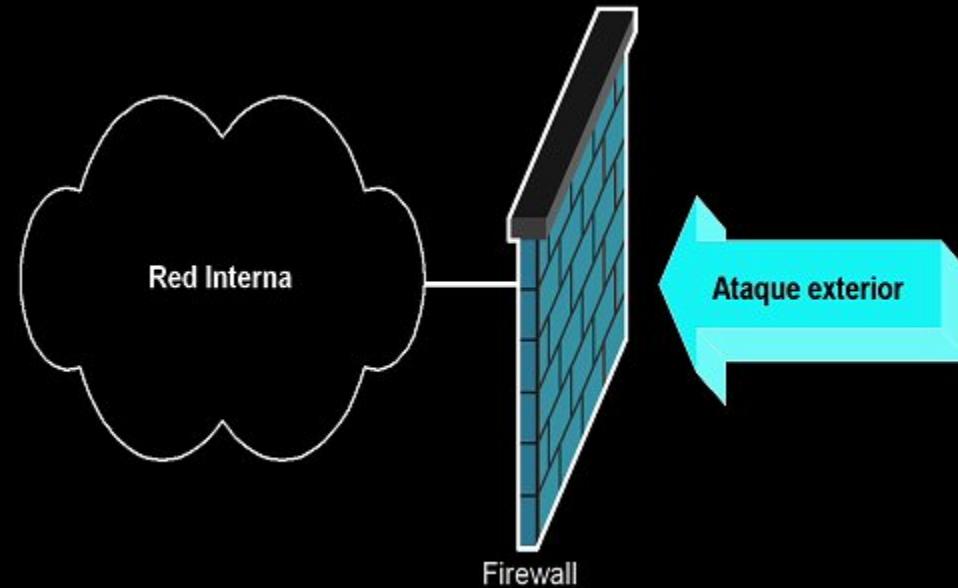
\$5,000 apiece for the training here.

[Read More](#)

[read comments \(0\)](#) | [write comment](#)



La seguridad no es...



!

- Ni un **firewall “tonto”** (*Filtrado Simple*)
- Ni tampoco un **Firewall “listo”** (*Filtrado de estados*).

Parte II

Políticas de seguridad



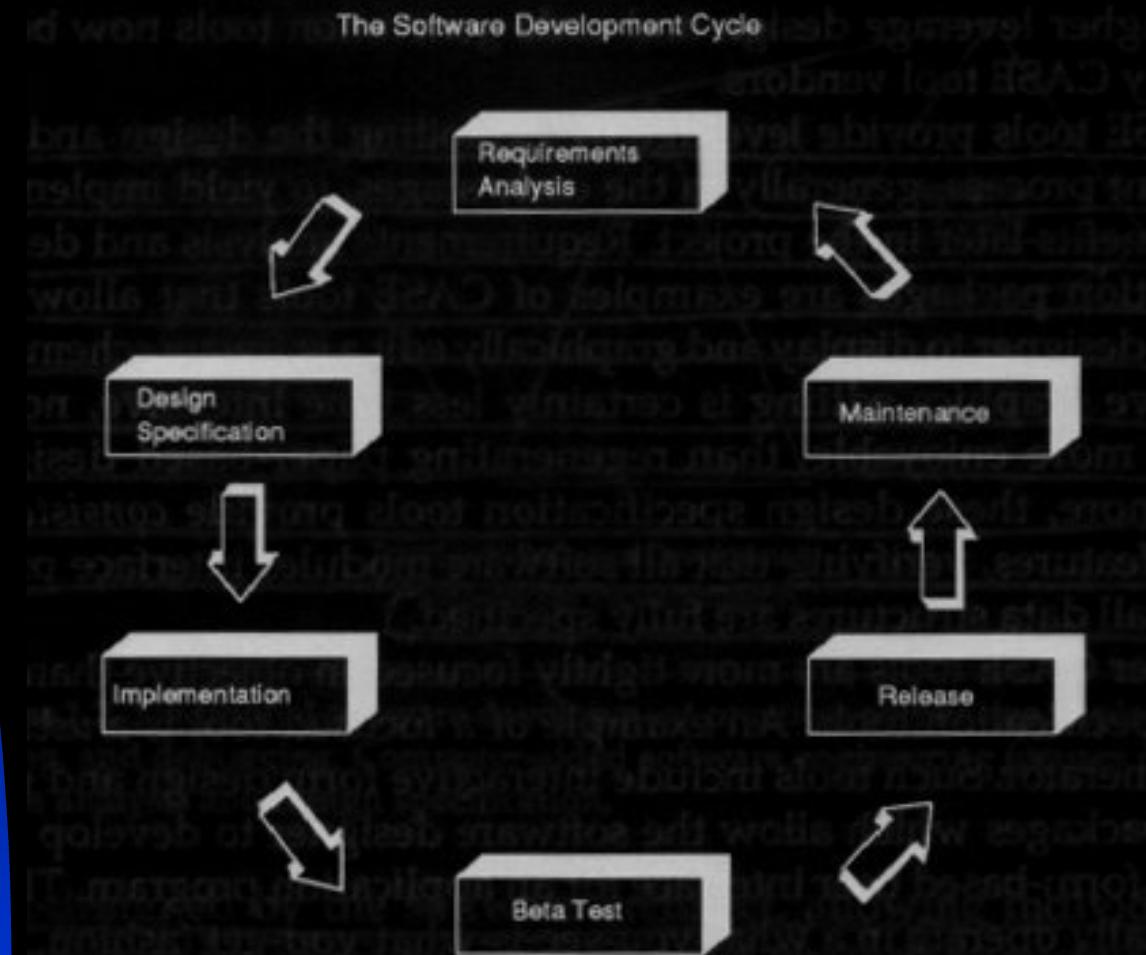
Ingeniería de Seguridad I

- Ingeniería de seguridad. Modelos
- Análisis
- Diseño
- Implementacion
- Mantenimiento e incidencias.
- Referencias.



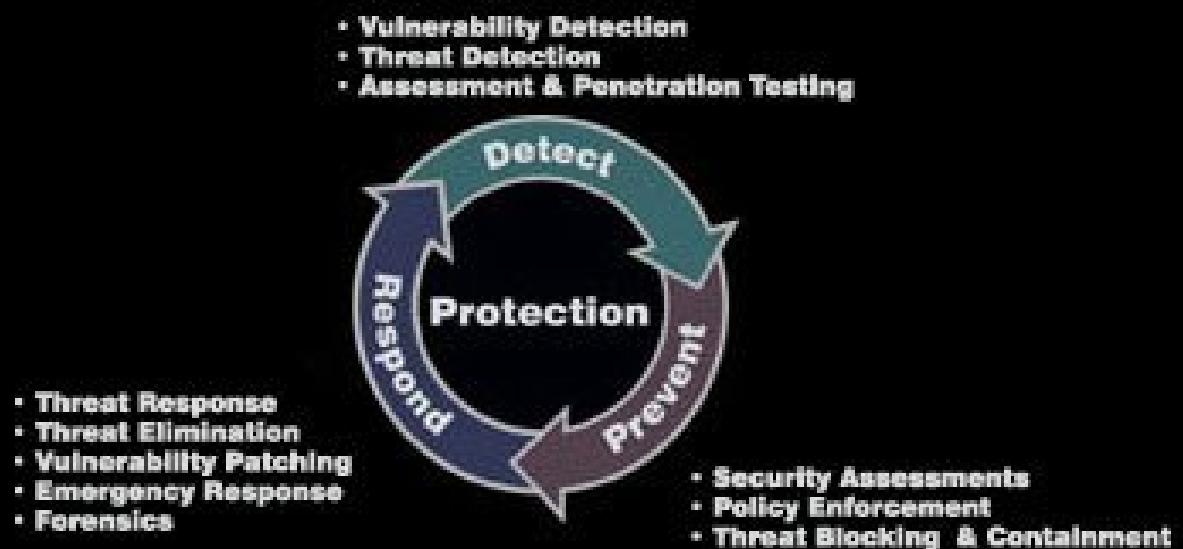
Ingeniería de Seguridad II

■ Modelo Clásico Ing. del Software



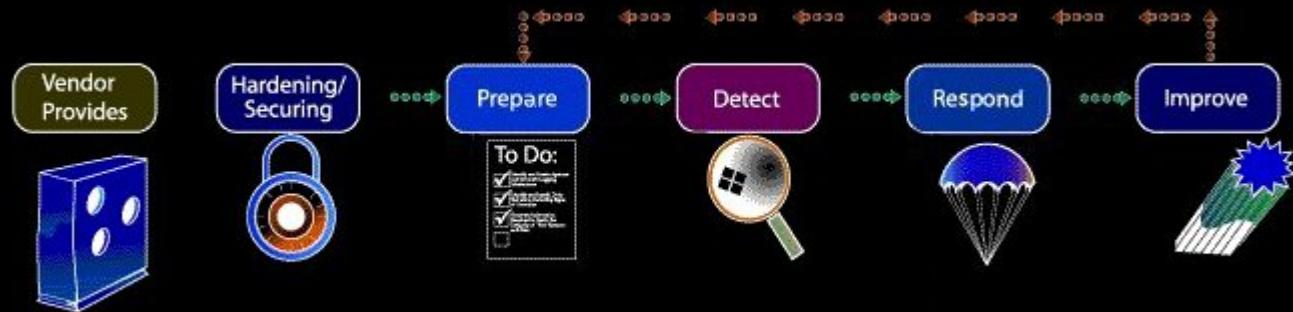
Ingeniería de Seguridad III

■ Modelo ISS



Fuente: ISS.net

Ingeniería de Seguridad IV



Fuente original: CERT.org

- Modelo CERT

Análisis. Que es (I)

■ Que es una Política de Seguridad

“La seguridad obtenida sólo con medios técnicos es limitada”,

“Sin técnica que la respalde, la seguridad es papel mojado”.

- ◆ Sistemas informaticos.

- ◆ Organizaciones.



Análisis. ¿ Que es ? (II)

- Una Política de Seguridad no es un firewall.
 - ◆ Fallos Tecnicos: Man in the middle, spoofing, autenticación débil...
 - ◆ Fallos no tecnicos: Señora de la limpieza, fallos humanos, mal diseño, poco control en la organización....
 - ★ Kevin Midnick



Análisis. ¿¡ QUE ES !? (III)

- ¿ Que es una política de seguridad ?
 - ◆ Confusiones varias al respecto.
 - ◆ Un conjunto de documentos, con un orden y una sistematización.
 - ◆ Describe paso a paso los distintos elementos de una política de seguridad.
 - ★ Detalla riesgos y peligros
 - ★ Como protegerse frente a esos riesgos, medidas a tomar y detalles de esas medidas.
 - ★ Que medidas tomar frente a posibles incidencias
 - ★ Que hacer en el peor de los casos



Análisis. Que es (IV)

- Una Política de Seguridad no se vende ni se compra.
 - ◆ No existen productos que hagan todo.
 - ◆ La seguridad se vende con el miedo.
 - ◆ El riesgo es real, las consecuencias diversas.
 - ◆ Figura del Consultor / Técnico de Seguridad.



Análisis. Necesidad

- Necesidad de una Política de Seguridad en una organización.
 - ◆ Confidencialidad.
 - ◆ Integridad.
 - ◆ Disponibilidad.



Análisis. Justificación

■ Justificación

- ◆ Establece lo que se puede hacer y lo que no, de forma escrita y formal. Se puede leer y es algo escrito y aceptado.
- ◆ Demuestra que la empresa se lo quiere tomar en serio. Implica un compromiso con los directivos.
- ◆ Util frente a una auditoria, sobre todo si se siguen las normalizaciones.
- ◆ Util para demostrar casos de intrusiones o delitos contra los sistemas informáticos.

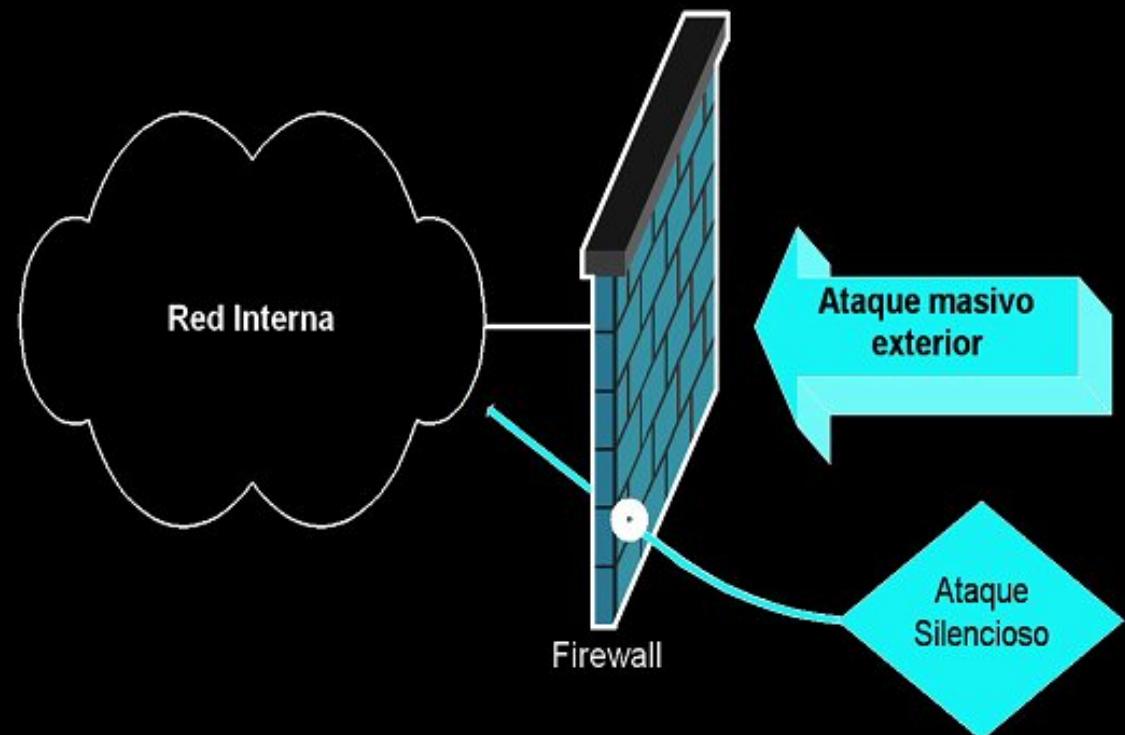


Analisis. Normalización I

- Normalización y método.
ISO 17799, BS7799, RFC 2196
 - ◆ Standard y certificación
 - ◆ Rigurosidad y Método
 - ◆ Hacking "ético"

Análisis. Normalización II

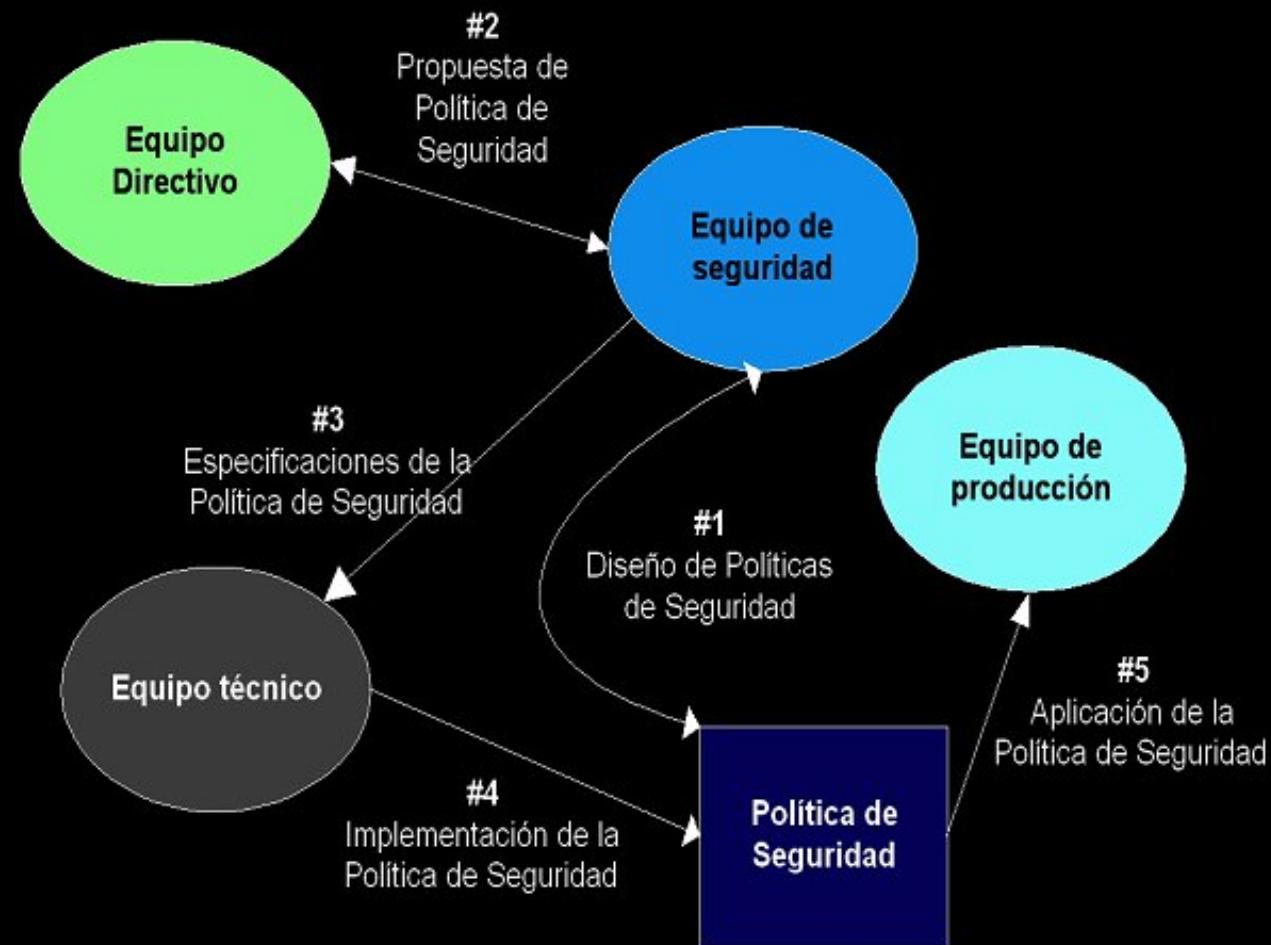
- Normalización y método II
 - ◆ Hacker vs Administrador
 - ★ Teoría de la “presa”



Análisis. Ámbitos

- Personas implicadas y responsabilidades en el proyecto.
 - ◆ Equipo de seguridad
 - ◆ Dirección de la organización
 - ◆ Personal técnico
 - ◆ Personal no técnico

Análisis. Ambitos (II)



Análisis. Riesgos (I)

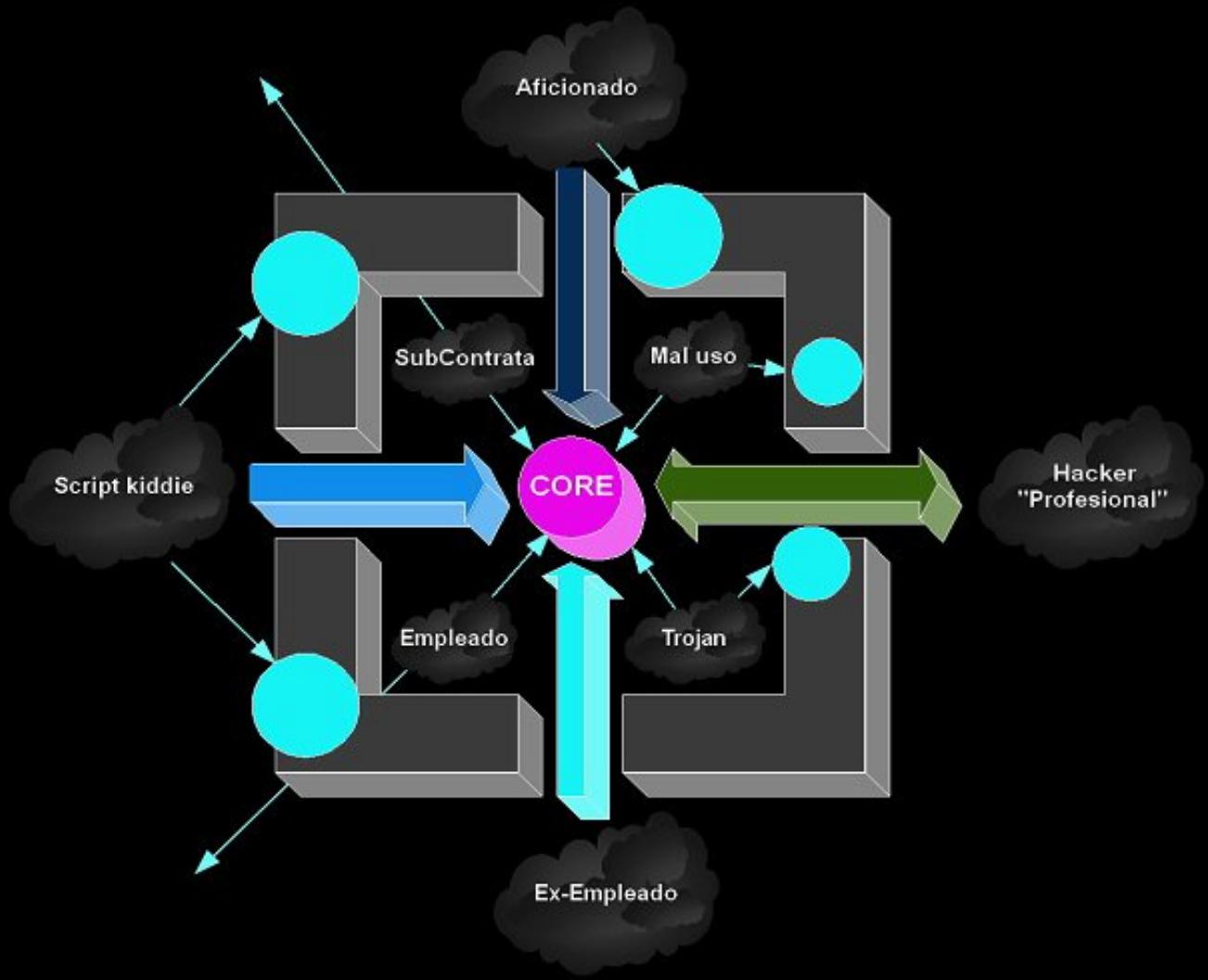
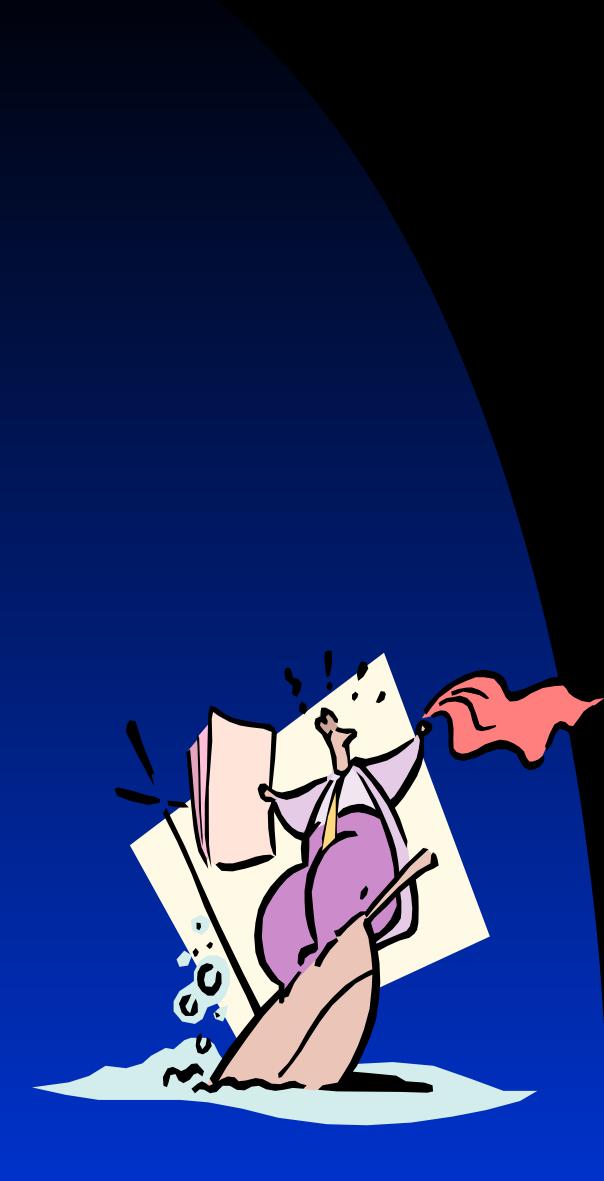
- Administrador vs Hacker. Teoria de la presa.
- Identificar peligros. Checklist.
 - ◆ Confidencialidad
 - ◆ Integridad
 - ◆ Disponibilidad
- Clasificación en niveles de seguridad. Normalizaciones.

Análisis. Riesgos (II)

■ ¿Que proteger?

- ◆ Acceso a Informacion comprometida o confidencial
 - ★ Planes de negocio, nominas, contratos, listados passwords, informacion de clientes.
- ◆ Acceso a Informacion valiosa
 - ★ Documentacion, desarrollos de I+D, historicos y archivos.
- ◆ Acceso a Inversiones e infraestructura
 - ★ Configuraciones, logs, backups, bbdd, webs, intranets, Acceso a servidores, electrónica y hardware costoso.

Análisis. Riesgos (III)



Análisis. Riesgos (IV)

■ Peligros contra la confidencialidad.

- ◆ Accesos no autorizados a información confidencial
- ◆ Accesos públicos a información confidencial, por error, mala configuración o descuido.
- ◆ Suplantación de usuarios.
- ◆ Acceso a servicios confidenciales (correo, bbdd, servidores de acceso, etc).
- ◆ Instalación de caballos de troya.
- ◆ Acceso físico a material restringido.

Análisis. Riesgos (V)

■ Peligros contra la integridad

- ◆ Modificación indebida de datos (fallo de permisos)
- ◆ Falta de integridad (borrado o modificación) de datos.
- ◆ Imposibilidad de identificar fuente de datos.
- ◆ Fallo en la integridad de bases de dato (corrupcion).
- ◆ Modificación en archivos de sistema (configuraciones, logs, etc)
- ◆ Destrucción o corrupción de backups.
- ◆ Virus.
- ◆ Acceso físico a material restringido.

Análisis. Riesgos (VI)

- Peligros contra la disponibilidad.
 - ◆ Caida de servicios externos. (DoS)
 - ◆ Agotamiento de recursos (ancho de banda, disco, socket, etc). (DoS o mala config.)
 - ◆ Fallo de infraestructuras generales de red (routing, switches, etc). (DoS, fallo, mala configuración o sabotaje)
 - ◆ Destrucción de configuraciones o servicios. (DoS o Sabotaje)
 - ◆ Acceso fisico a infraestructura básica. Sabotaje.

Análisis. Riesgos (VII)

- DoS
 - ◆ Casos historicos: Yahoo, Amazon, eBay, etc. Perdidas.
 - ◆ Tecnicas varias.
 - ★ Fallos especificacion protocolo.
 - ★ Programacion deficiente (buffer overflow).
 - ★ Flood.
 - ★ Acceso a los servicios: Fuerza bruta, trojan, otros.
 - ★ Spoofing vario (IP, DNS, etc).
 - ★ Session hijacking.
 - ★ Ingenieria social y acceso fisico.
 - ★ DDoS y gusanos

Análisis. Riesgos (VII)

- Resumen de riesgos:
 - ◆ Acceso a información sensible.
 - ◆ DoS y fallos de programación.
 - ◆ Mal uso de recursos.
- ¿ Era un firewall suficiente ?
- ¿ Existe algo suficiente por si mismo para garantizar la seguridad ?

Diseño. Introducción

- Diseño.
 - ◆ Como llevar esto a la práctica
- Uso de herramientas
 - ◆ ISO 17799 y BS 7799
 - ◆ RFC 2196
 - ◆ Orange Book (DoD EEUU)
 - ◆ CERT Security Guidelines
 - ◆ Otras guías

Diseño. Vamos allá (I)

- Organizando subpolíticas
- Las mas importantes y comunes
 - ◆ Uso de los recursos del sistema (*)
 - ◆ Política de cuentas de usuario (*)
 - ◆ Política de protección de la información (*)
 - ◆ Política legal (*)
 - ◆ Política de seguridad general de los sistemas informáticos en producción (*)
 - ◆ Política de backup (*)
 - ◆ Política de control de accesos (*)
 - ◆ Política de accesos y permisos (*)
 - ◆ Política de seguridad física (*)



Diseño. Vamos allá (II)

■ Otras subpolíticas.

- ◆ Política de Accesos remotos.
- ◆ Política de educación en el ámbito de la seguridad.
- ◆ Política de prevención y detección de virus.
- ◆ Plan de continuidad de negocio.
- ◆ Política de passwords.
- ◆ Política de seguridad perimetral de los sistemas informáticos.

Diseño. Vamos allá (III)

■ Otras subpolíticas (continuación)

- ◆ Política de seguridad perimetral interna de los sistemas informáticos.
- ◆ Política de intervenciones.
- ◆ Política de incidencias.
- ◆ Política de alta disponibilidad y redundancia.
- ◆ Política de guardias 24x7
- ◆ Política de gestión de recursos informáticos.
- ◆ Política de monitorización.
- ◆ Política de encriptación y ocultación de información.

Parte III

Implementación



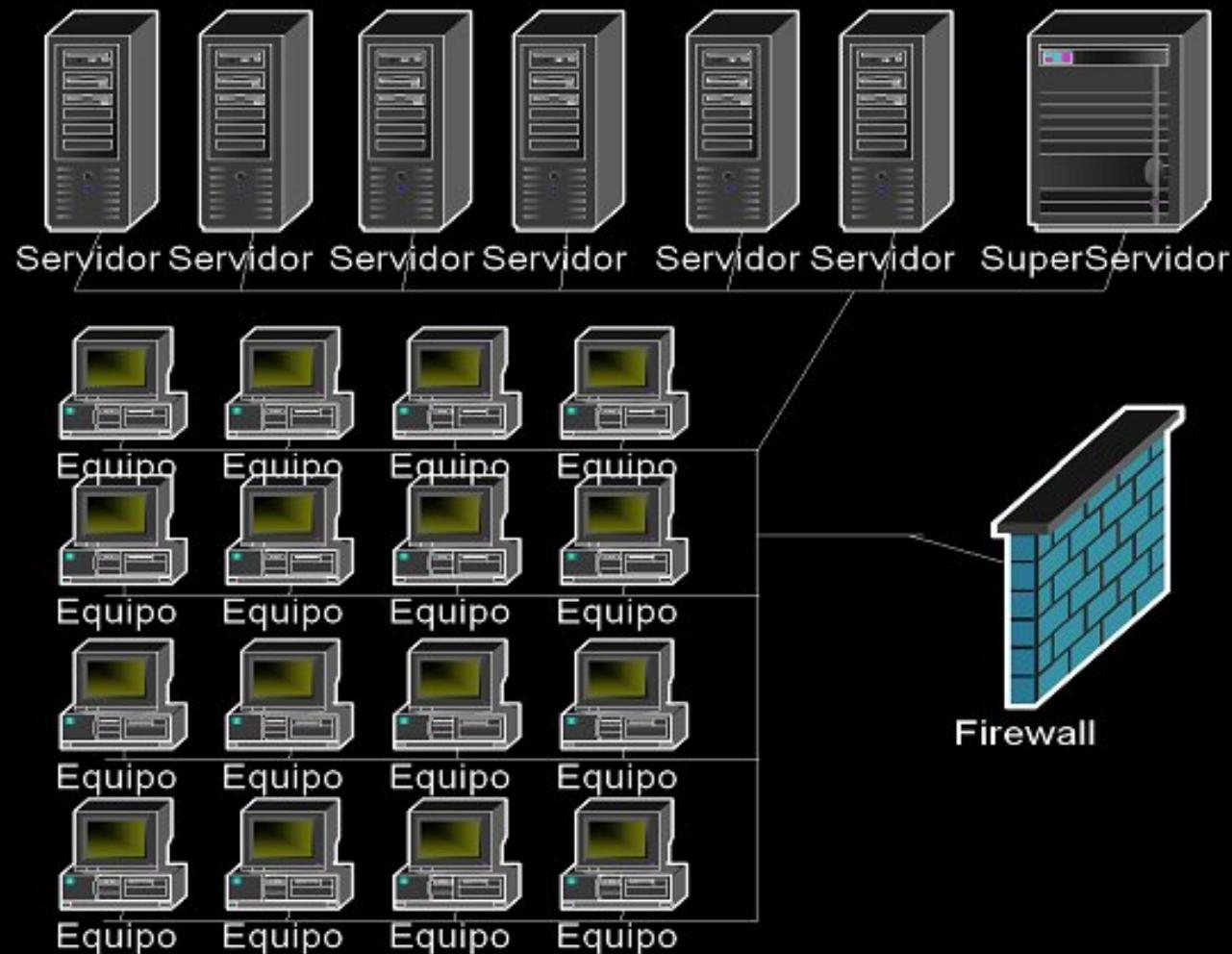
Implementación

■ De qué partimos

- ◆ Buenos conocimientos de sistemas.
- ◆ Sólidos conocimientos de TCP/IP.
- ◆ Teoría de SSOO, redes, y algo de programación.

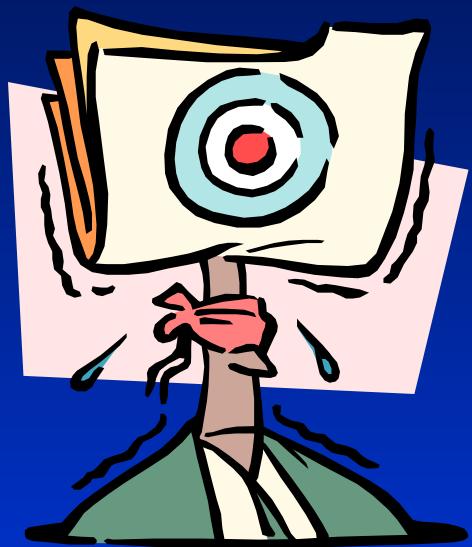
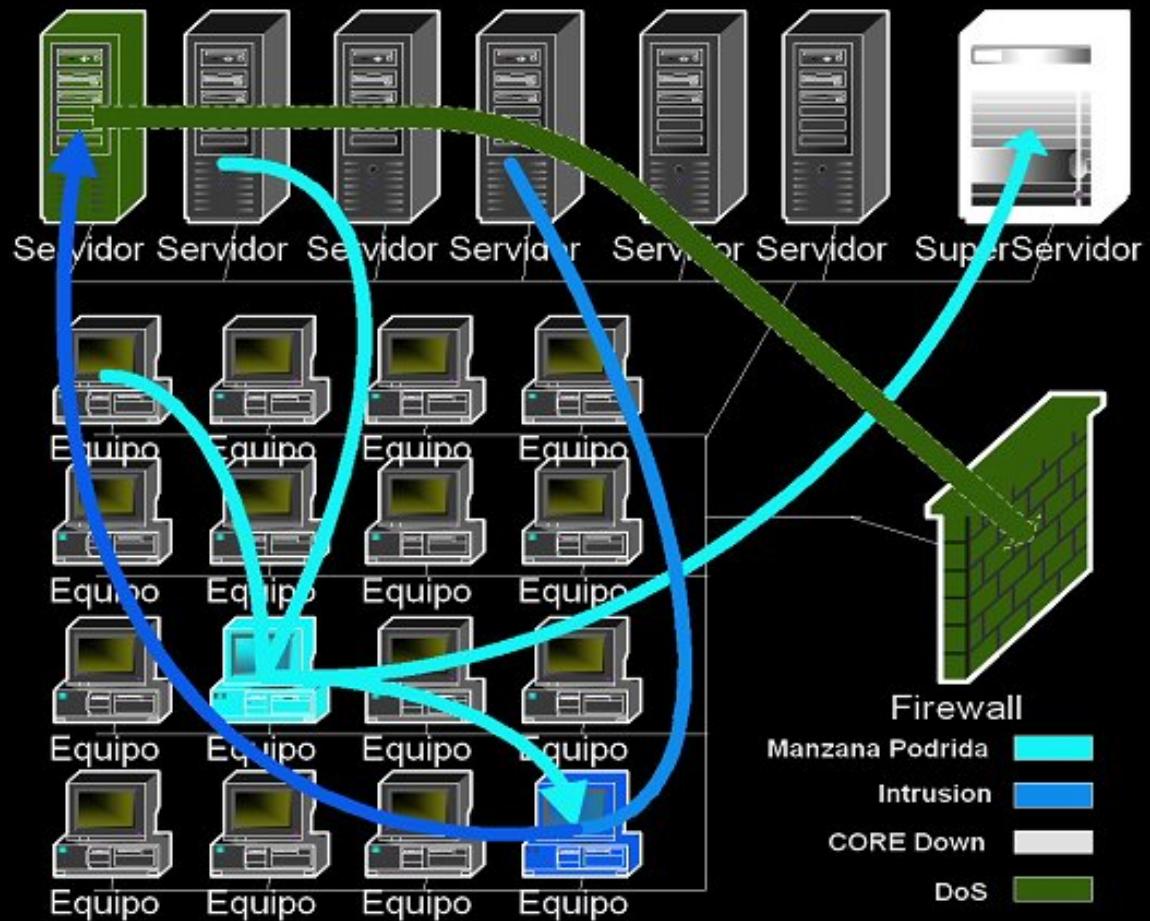


Implementacion: Compartimentación de redes



Compartimentación de redes II.

- Manzana podrida

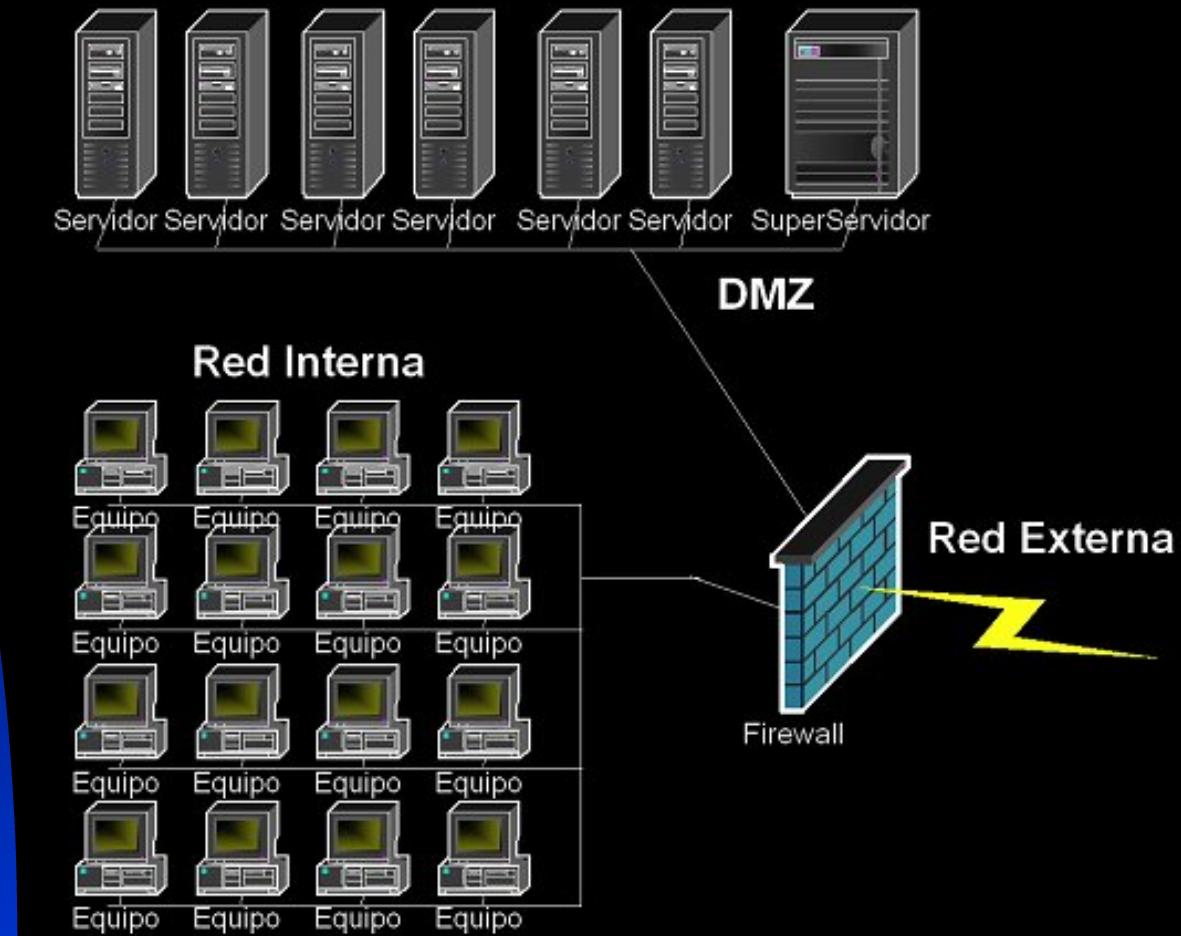


Compartimentacion de redes III

- Diferenciar las redes logicamente por su funcion y su nivel de seguridad.
- Diferenciar las redes fisica y lógicamente.
- Modelos
 - ◆ Simple: DMZ
 - ◆ Complejo: FrontEnd y BackEnd

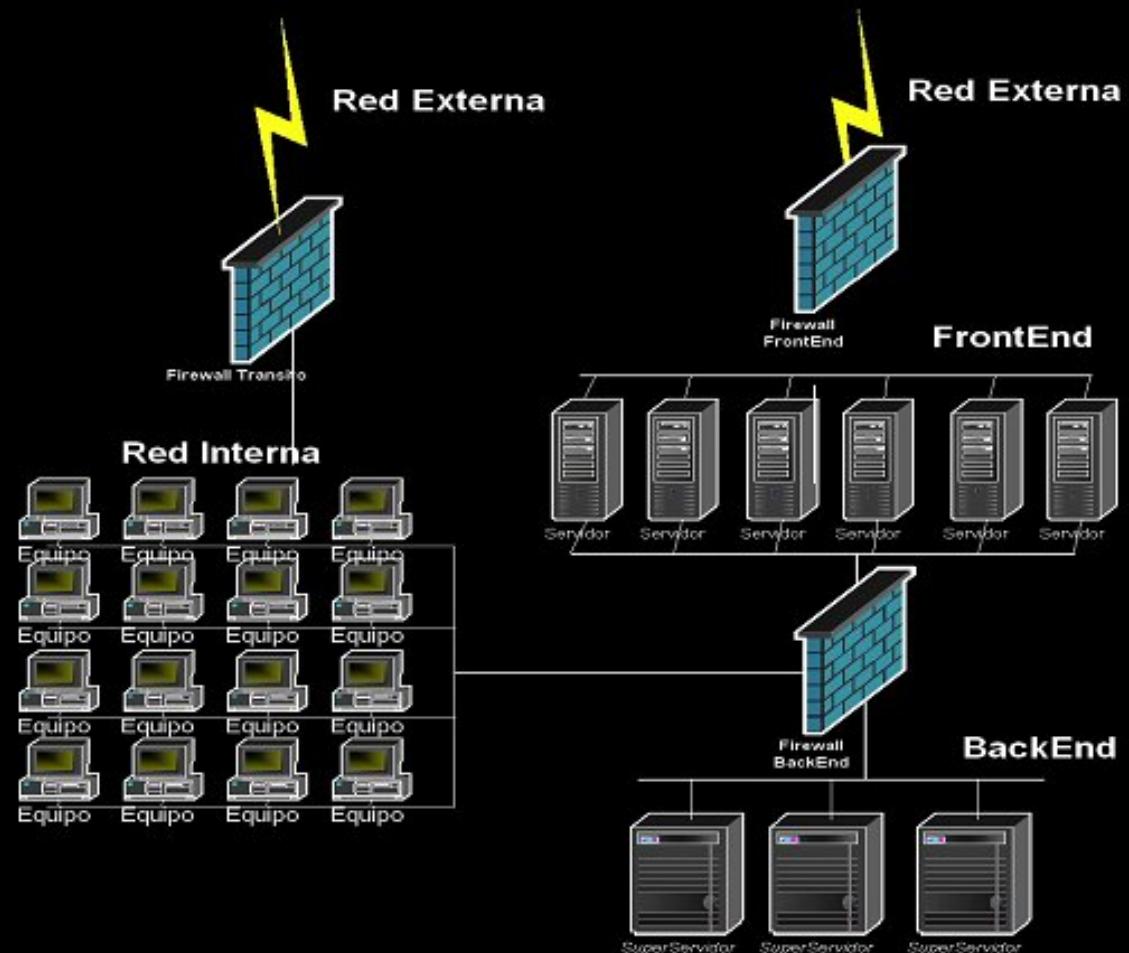
Compartimentacion de redes IV

- Modelo clásico: DMZ



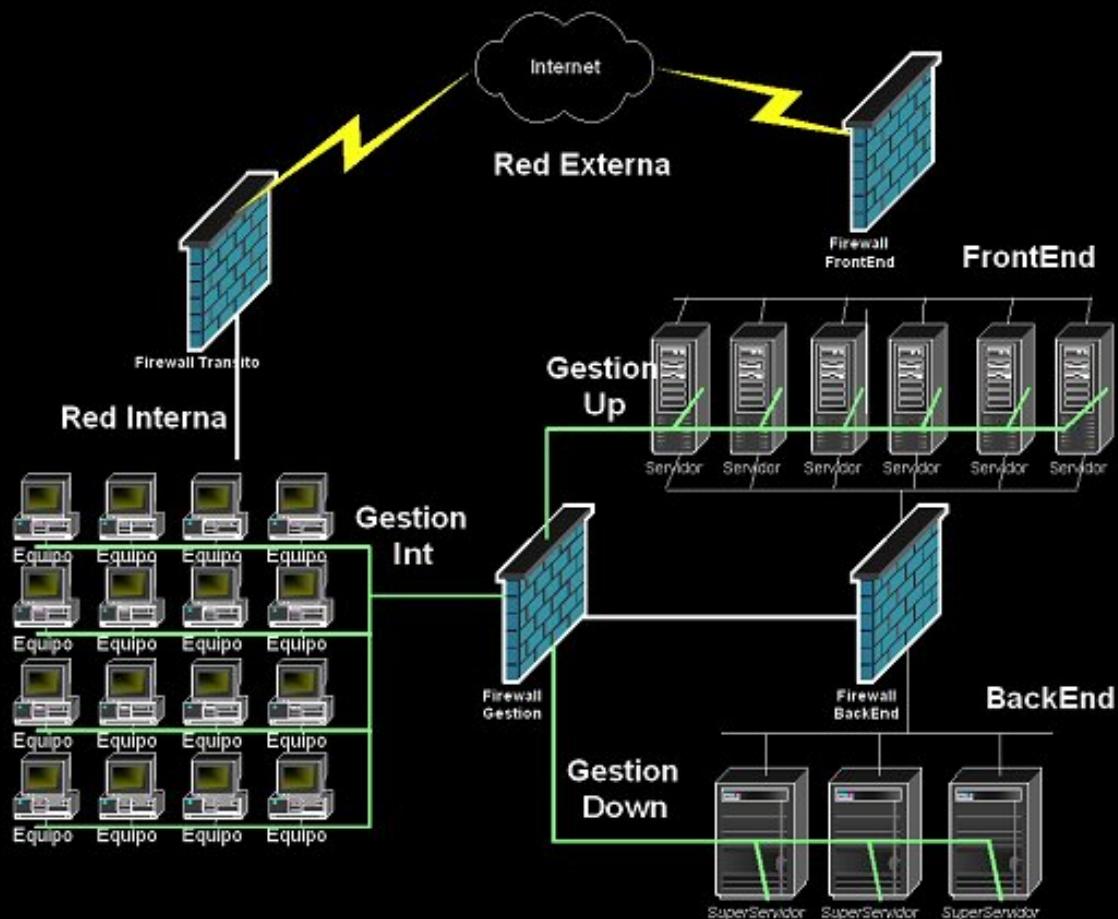
Compartimentacion de redes V

- Modelo complejo. FE y BE (fase 1)



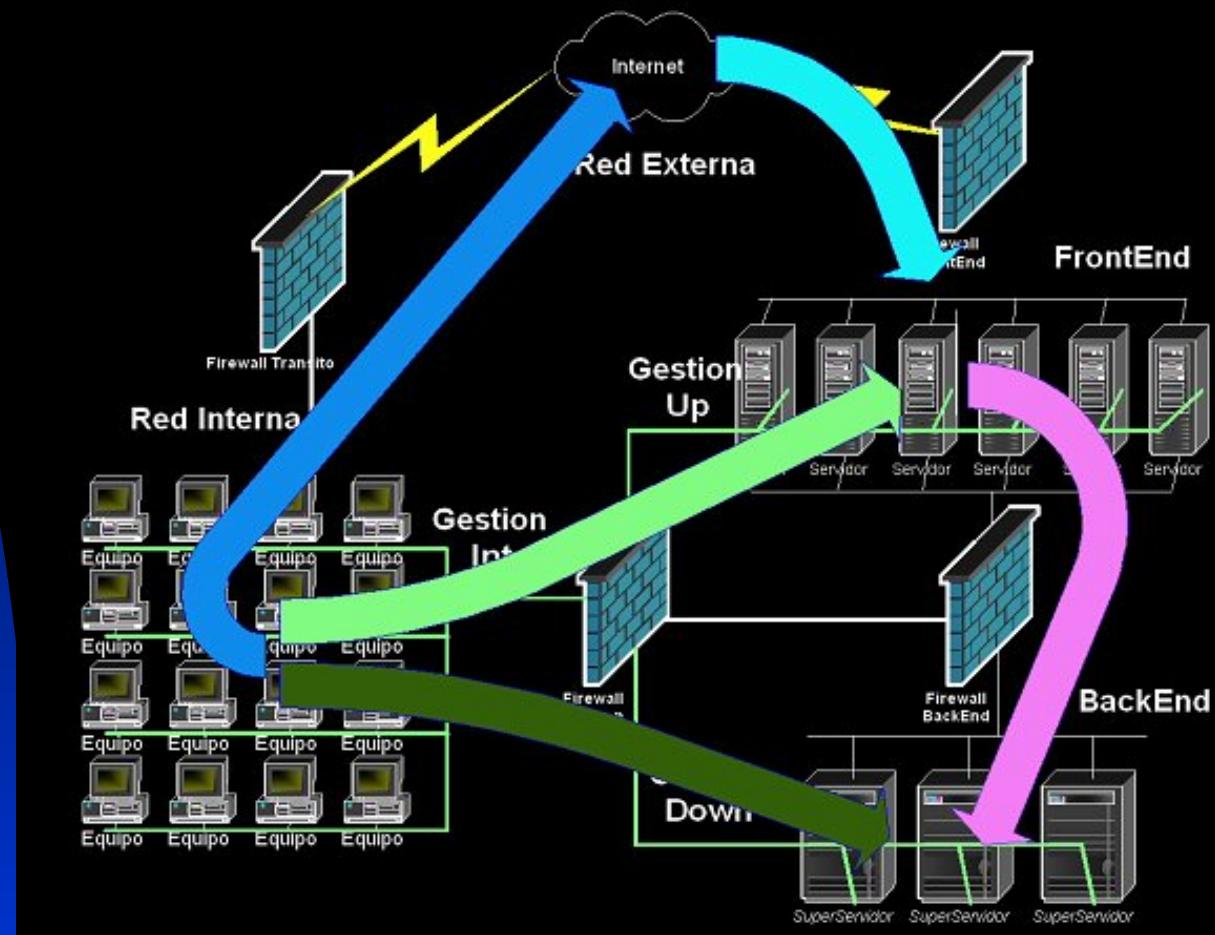
Compartimentacion de redes VI

- Modelo complejo. FE y BE (fase 2)



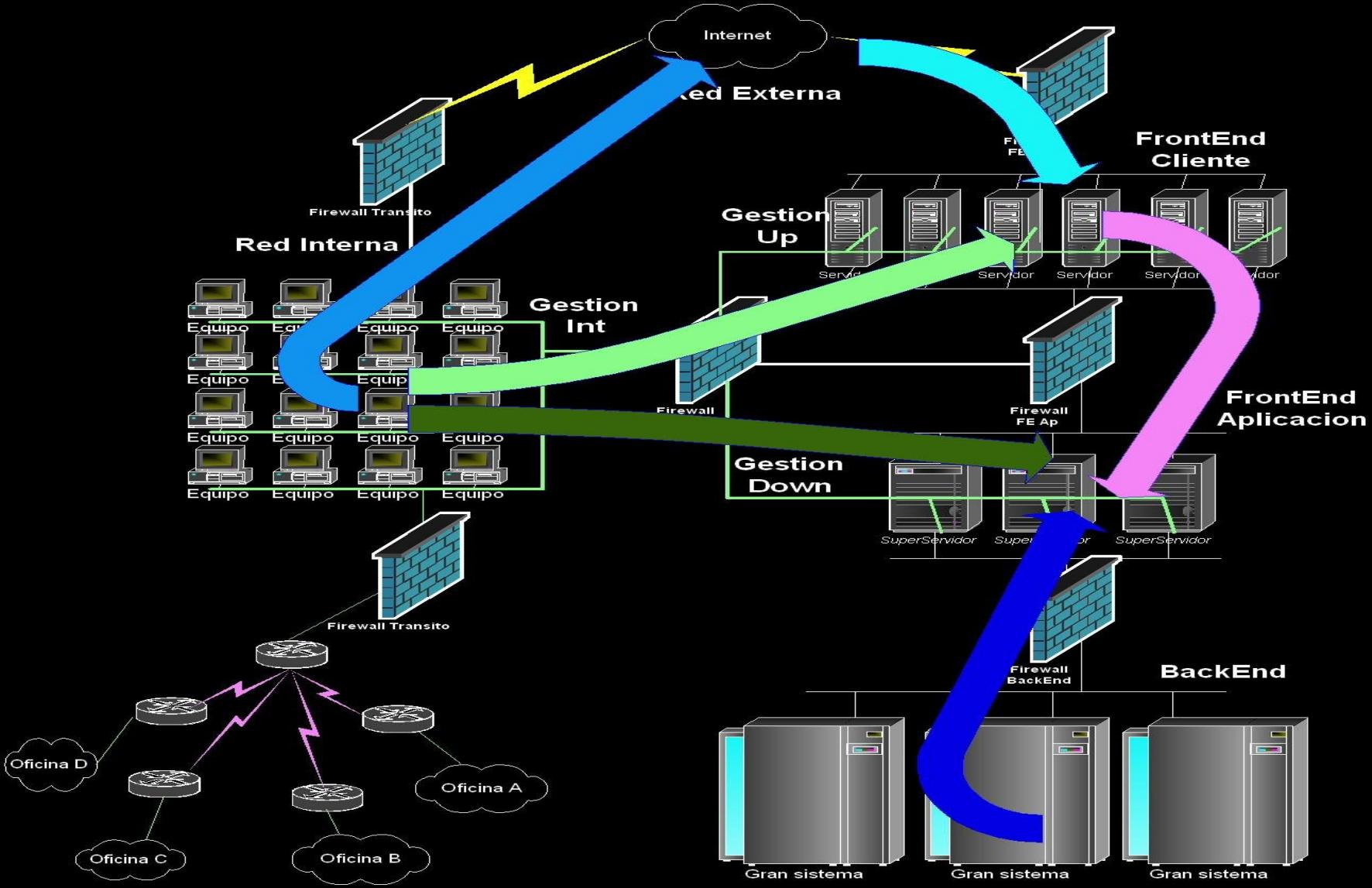
Compartimentacion de redes VII

- Flujos en el modelo complejo



Compartimentacion de redes VIII

- Modelo complejo. FE v BE (fase 3)



Implementacion. Netfilter

- Qué es un firewall
- Qué tipos de firewall hay
- Netfilter en Linux
- HA con Netfilter
- Utilidades con Netfilter
- Configurando Netfilter

Implementacion. Netfilter II

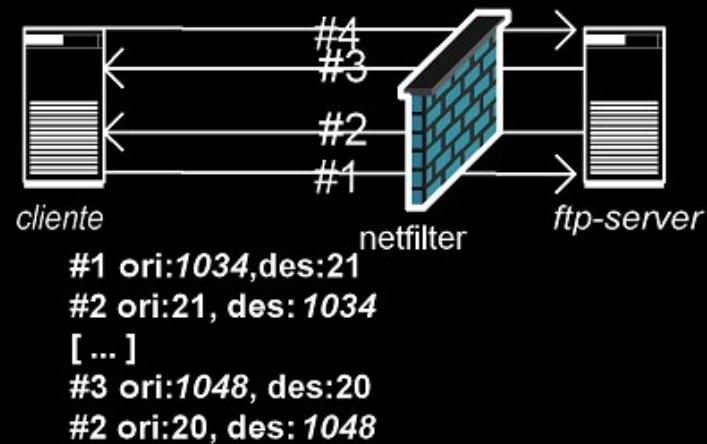
- Qué es un firewall
 - ◆ Necesidad de un firewall
 - ◆ Funcionamiento de un firewall
- Que tipos de firewall hay
 - ◆ Filtrado básico o tonto
 - ◆ Filtrado inteligente o de inspección de estados
 - ◆ Proxys y Firewalls de aplicación

Implementacion. Netfilter III

- ◆ Filtrado básico o tonto



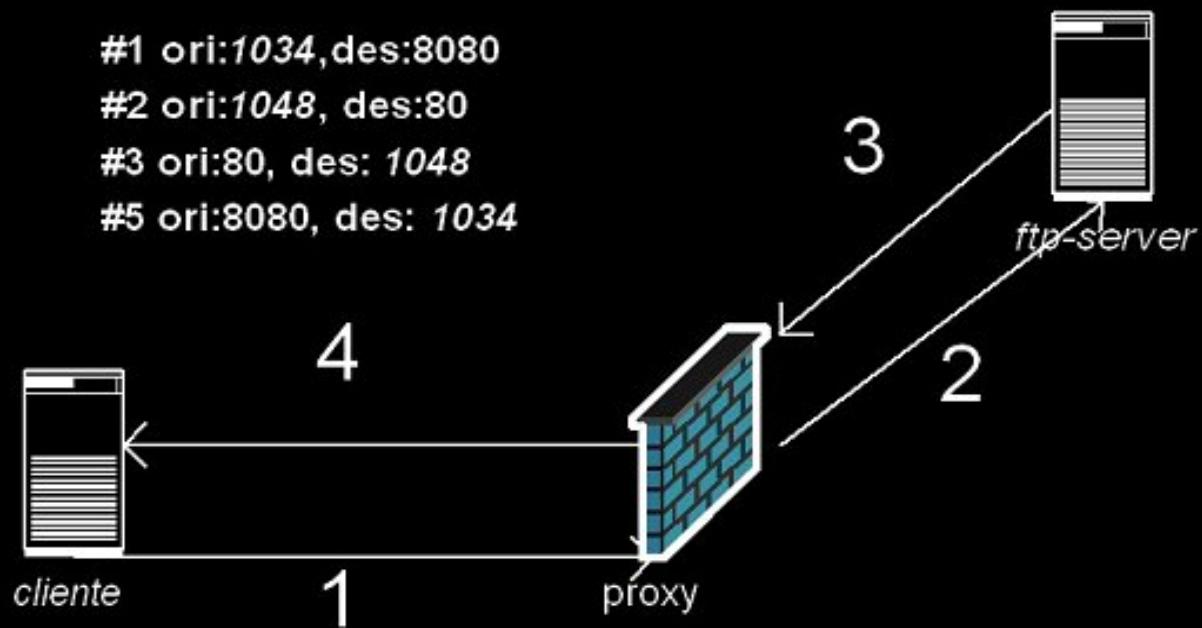
- ◆ Filtrado inteligente o de inspección de estados



Implementacion. Proxys

- Proxys y Firewalls de aplicación
 - ◆ Squid
 - ◆ Proxy Socks

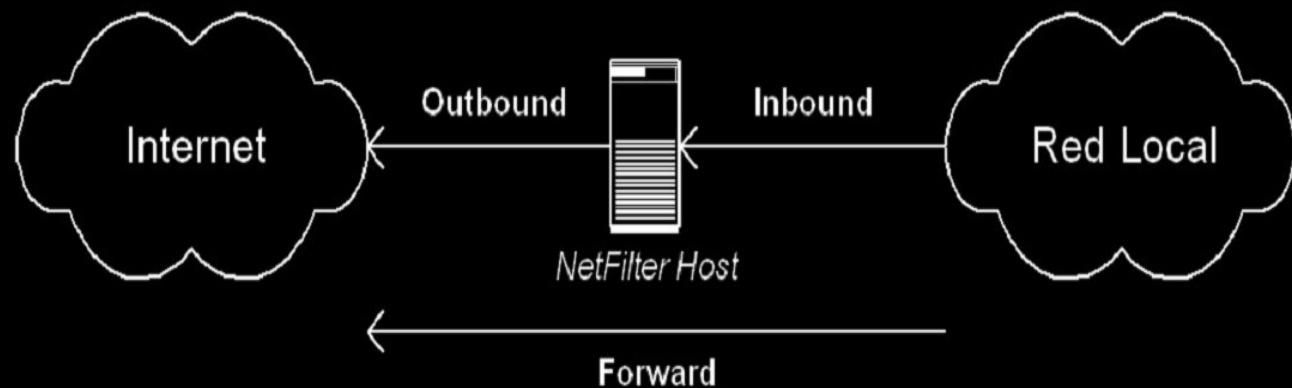
```
#1 ori:1034,des:8080  
#2 ori:1048, des:80  
#3 ori:80, des: 1048  
#5 ori:8080, des: 1034
```



Implementación. Cadenas

■ Cadenas

- ◆ Organizar flujos
- ◆ Orden de ejecucion
- ◆ Jerarquizacion



Implementación. Cadenas II

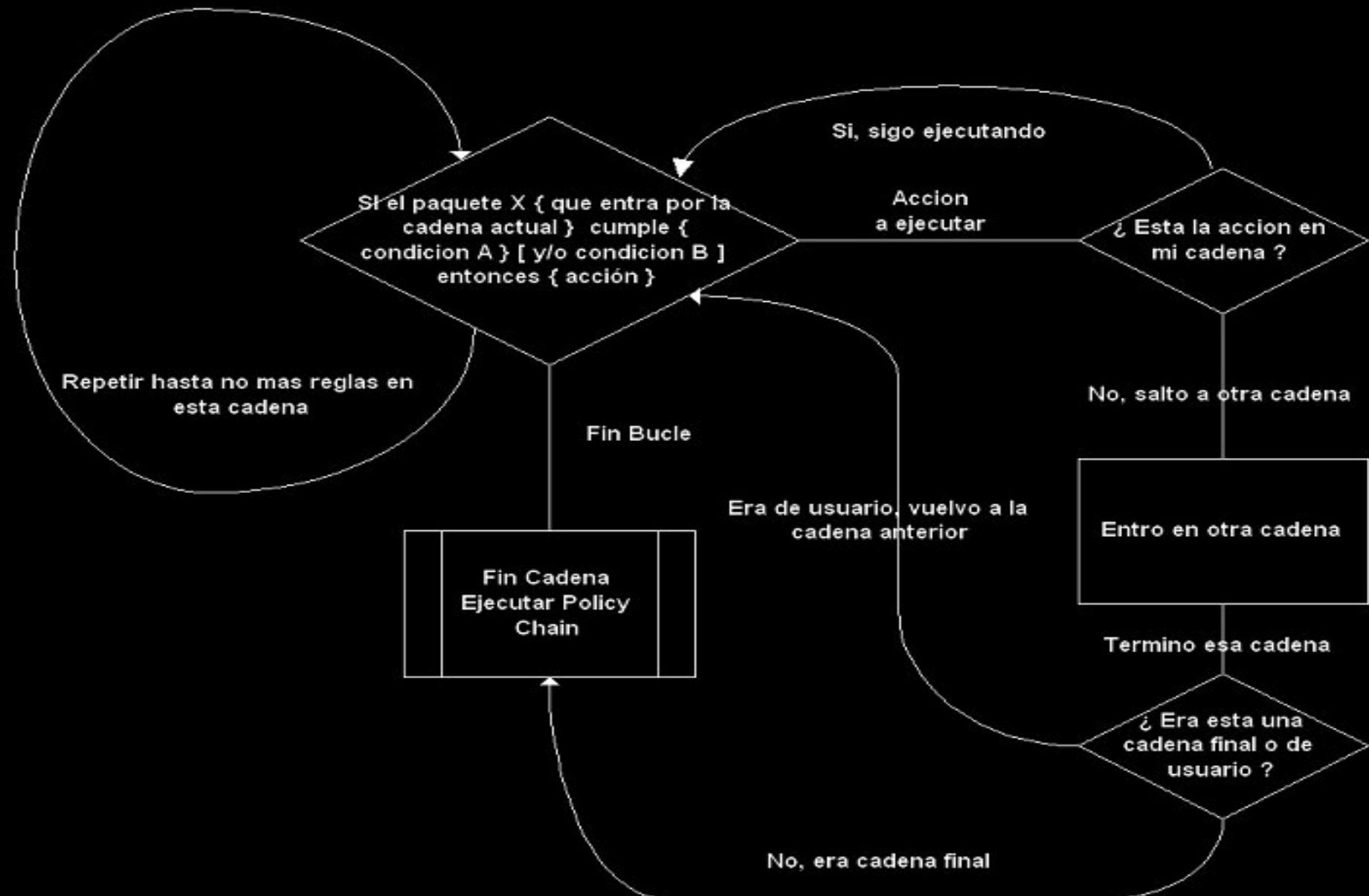
■ Cadenas Destino/Acción

- ◆ Accept
- ◆ Drop
- ◆ Reject
- ◆ Log
- ◆ Prerouting
- ◆ PostRouting
- ◆ Masquerade

Implementación. Cadenas III

- Encadenando otras cadenas
- Cadenas de usuario
- Recursión

Implementación. Cadenas IV



Implementación. Cadenas V

■ Sintaxis, #iptables

- N**, --new-chain <nombre_de_cadena>, crearemos una cadena.
- X** <nombre_de_cadena>, borramos una cadena.
- I**, --insert <nombre_de_cadena> { regla } , insertamos una regla al *principio* de una cadena.
- A**, --append <nombre_de_cadena> { regla } ,insertamos una regla al *final* de una cadena.
- D**, --delete <nombre_de_cadena> {# | regla } , borramos una regla de la cadena dada. Podemos especificar la posición (1, 2 ..) o la regla en formato convencional.
- R**, --replace <nombre_de_cadena> { # regla } ,reemplazamos una regla de la cadena especificada. Hay que especificar el numero de la cadena que queremos reemplazar y luego la regla a introducir.
- L**, --list <nombre_de_cadena>, lista todas las reglas pertenecientes a la cadena dada.
- F**, --flush , elimina todas las reglas, es lo mismo que eliminar todas las reglas una por una.

Implementación. Iptables

- Sintaxis general
 - ◆ Opciones (limit burst)
 - ◆ Modularidad

```
Iptables -I|-A <cadena> -I <ifaz> -p <tcp|udp>
          --sport|--dport [!] <puerto>|<rango-rango>
          -d [!] <ip> -s [!] <ip> -m <modulo>
          --from <IP_SNAT> --to <IP_DNAT>
          -j <destino>
```

Implementación. Filtrado I

■ Filtrado

- ◆ Por direcciones
- ◆ Por puertos (TCP, UDP, ICMP)
- ◆ Por interfaz
- ◆ Por rafagas
- ◆ Por bits de cabecera

Implementación. Filtrado II

- ¿Dónde filtramos?
 - ◆ Input, o hacia el firewall
 - ◆ Output, o desde el firewall
 - ◆ Forward, o lo que pasa por el firewall.

```
# iptables -I|-A INPUT|OUTPUT|FORWARD
```

Implementación. Filtrado III

■ Como filtrar, algunos ejemplos:

```
iptables -A FORWARD -d POLLUX -p tcp --dport 22      -j ACCEPT # SSH  
iptables -A FORWARD -d POLLUX -p tcp --dport 23      -j ACCEPT # FTP  
iptables -A FORWARD -s POLLUX -i eth1 -j ACCEPT  
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT  
iptables -P FORWARD DROP
```

```
iptables -A INPUT -s PRIVATE -p tcp --dport 22      -j ACCEPT # SSH  
iptables -A OUTPUT -d PRIVATE -p tcp --sport 22 -J ACCEPT # SSH out  
iptables -P INPUT DROP  
iptables -P OUTPUT DROP
```

Implementacion. NAT

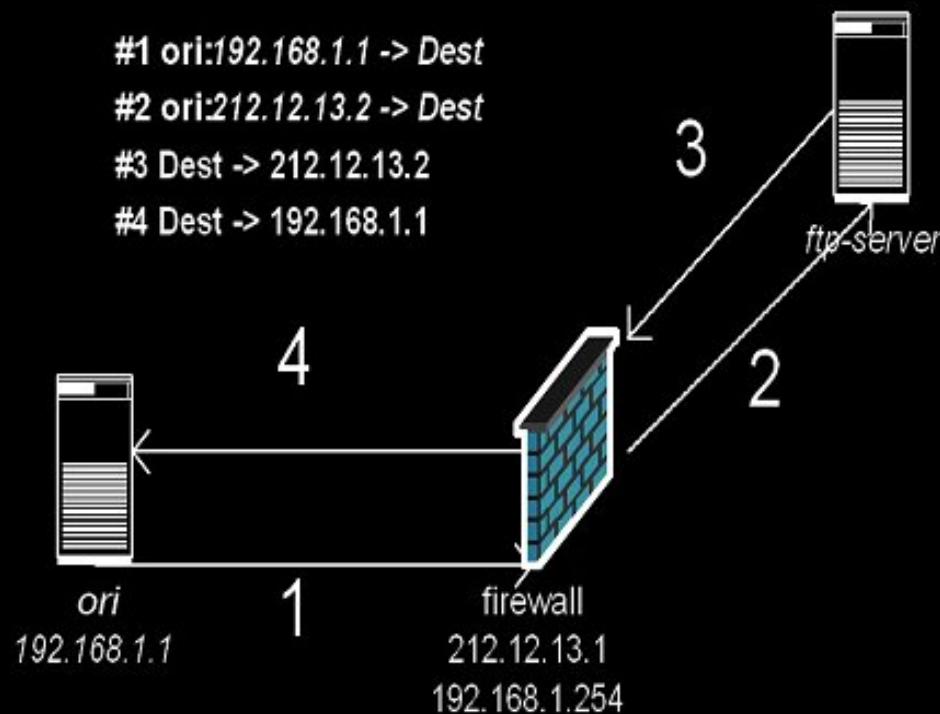
- Network Address Translation
 - ◆ Necesidad
 - ★ Escasez IP's
 - ★ Ocultación direccionamiento
 - ★ Port Multiplexing
 - ★ Flexibilidad
 - ◆ Tipos
 - ★ NAT de IP
 - ★ NAT de Puertos (PAT)

Implementacion. NAT II

- Network Address Translation
 - ◆ Tipos de NAT.
 - ★ Descripcion sobre variedades
 - Port Forwarding, Dynamic Nat, Smart NAT, Intelligent NAT, Dinamic NAT, Hide NAT, Static NAT, Masquerading y otras disparidades.
 - ★ Source NAT
 - ★ Dynamic NAT/Masquerading
 - ★ Destination NAT

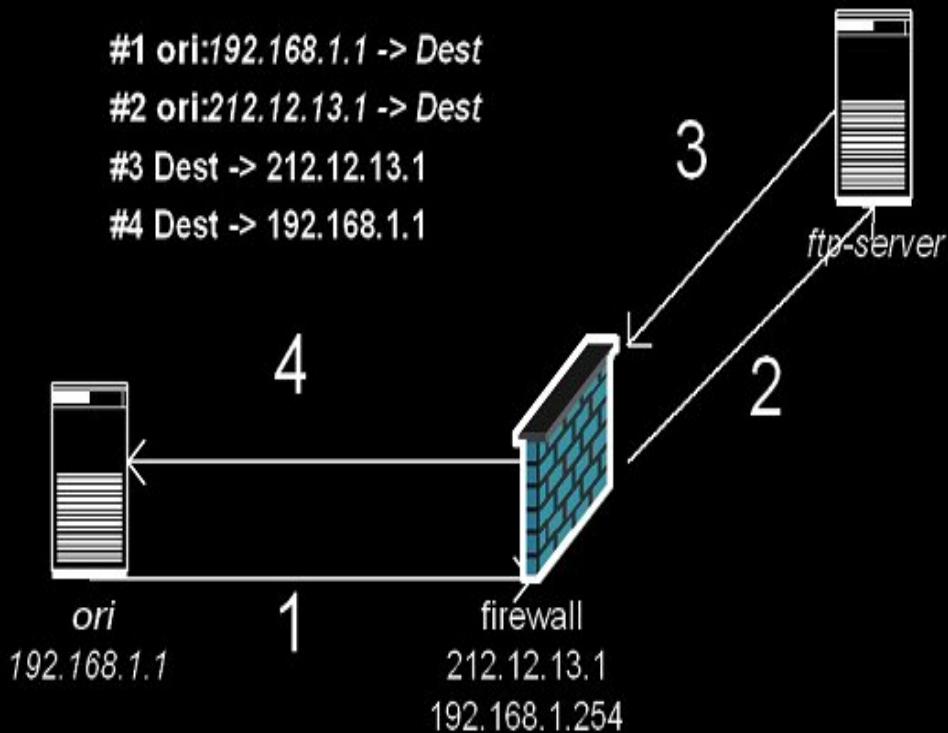
Implementacion. SNAT

■ Source NAT



Implementacion. SNAT II

- Masquerading, Dynamic SNAT

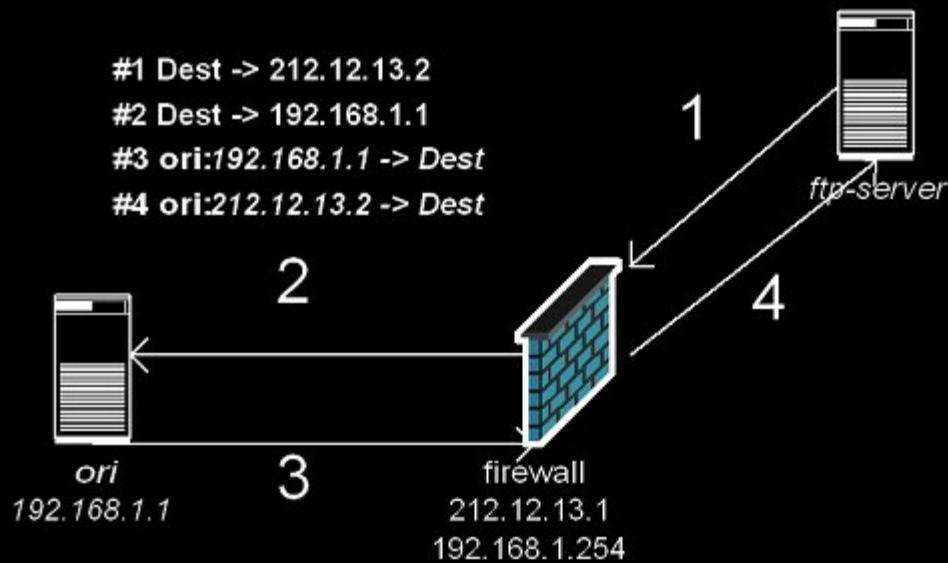


Implementacion. DNAT

- Destination NAT (DNAT)
 - ◆ Necesidad e importancia
 - ◆ Funcionamiento básico
 - ◆ Formas de implementarlo
 - ◆ Algoritmo de entrega ethernet/ip
 - ◆ Routing
 - ◆ Proxy ARP

Implementacion. DNAT II

- DNAT. La idea
 - ◆ ¿De donde sacamos esa IP?
 - ◆ IP Virtual en Firewall

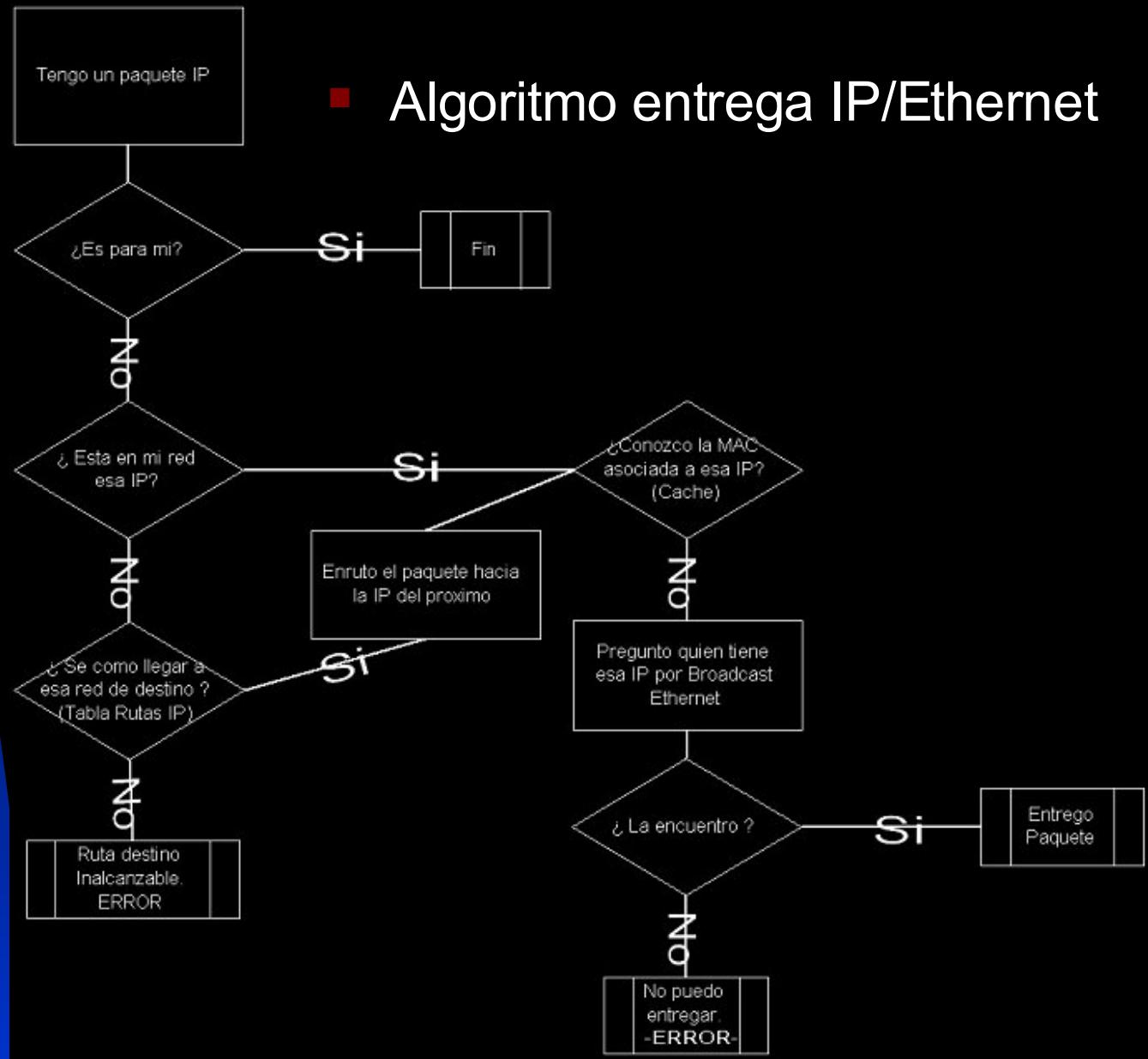


Implementacion. DNAT III

- Algoritmo de entrega Ethernet/IP
 - ◆ ¿Esta la IP en mi ruta?
 - ◆ Entrega ETHERNET
 - ★ Capa L2
 - ◆ Broadcast IP
 - ◆ Broadcast Ethernet
 - ★ Ejemplos broadcast otros protocolos (ATM)

Implementacion. DNAT IV

■ Algoritmo entrega IP/Ethernet



Implementacion. DNAT V

■ DNAT con Enrutamiento L3

#1 Dest -> 212.12.13.2 via 212.12.13.254

#1' 212.12.13.254(Dest) -> 212.12.13.2 via 212.12.13.254

DNAT in ("Manual")

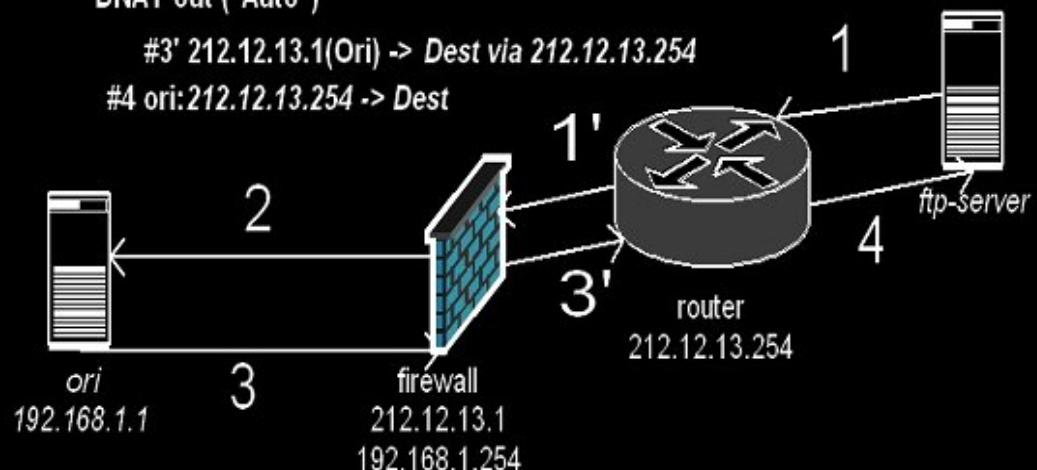
#2 192.168.1.254(Dest) -> 192.168.1.1

#3 ori:192.168.1.1 -> Dest via 192.168.1.254

DNAT out ("Auto")

#3' 212.12.13.1(Ori) -> Dest via 212.12.13.254

#4 ori:212.12.13.254 -> Dest



Implementacion. DNAT VI

- DNAT con Enrutamiento L2.
Proxy ARP

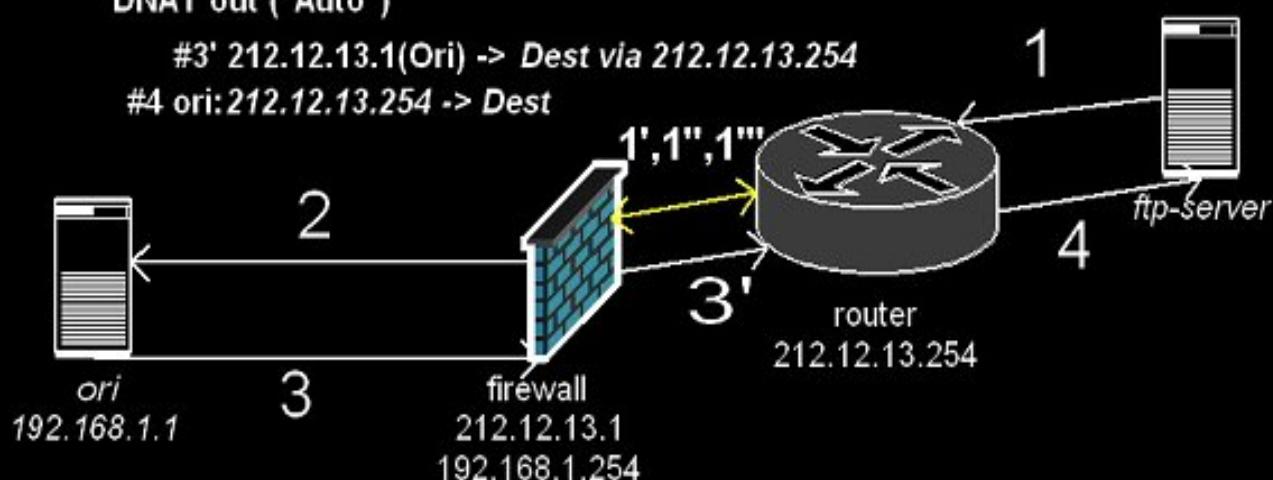
```
#1 Dest -> 212.12.13.2 via 212.12.13.254  
#1' 212.12.13.254 ask -> Who has 212.12.13.2?  
#1" 00:0A:B8:C0:E1:03 reply -> I'm 212.12.13.2  
#1'" 212.12.13.254(Server) -> 212.12.13.2 via 00:0A:B8:C0:E1:03
```

DNAT in ("Manual")

```
#2 192.168.1.254(Dest) -> 192.168.1.1  
#3 ori:192.168.1.1 -> Dest via 192.168.1.254
```

DNAT out ("Auto")

```
#3' 212.12.13.1(Ori) -> Dest via 212.12.13.254  
#4 ori:212.12.13.254 -> Dest
```



Implementacion. DNAT VII

- DNAT con Enrutamiento L3,
implementacion con linux.
 - ◆ Hay que hacerlo en el punto intermedio (router)
 - ◆ A veces no tenemos acceso

```
# route add 212.12.13.2 gw 212.12.13.1
```

Implementacion. DNAT VIII

- DNAT con Enrutamiento L2. Proxy ARP, implementacion con linux
 - ◆ Determinar la MAC externa

```
# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 52:54:4C:03:E4:CD
          inet addr:212.12.13.1    Bcast:217.126.145.192
eth1      Link encap:Ethernet  HWaddr 00:A0:C9:4C:F9:09
          inet addr:192.168.1.254  Bcast:192.168.1.255
```

- ◆ Meter ruta estatica ARP

```
#arp -s 212.12.13.2 52:54:4C:03:E4:CD pub
```

Implementacion. DNAT IX

- DNAT con Enrutamiento L2. Proxy ARP, implementacion con linux.
 - ◆ Determinar la MAC externa

```
# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 52:54:4C:03:E4:CD
          inet addr:212.12.13.1    Bcast:217.126.145.192
eth1      Link encap:Ethernet  HWaddr 00:A0:C9:4C:F9:09
          inet addr:192.168.1.254  Bcast:192.168.1.255
```

- ◆ Meter ruta estatica ARP

```
#arp -s 212.12.13.2 52:54:4C:03:E4:CD pub
```

Implementacion. NAT X

■ Reglas de NAT, ejemplos.

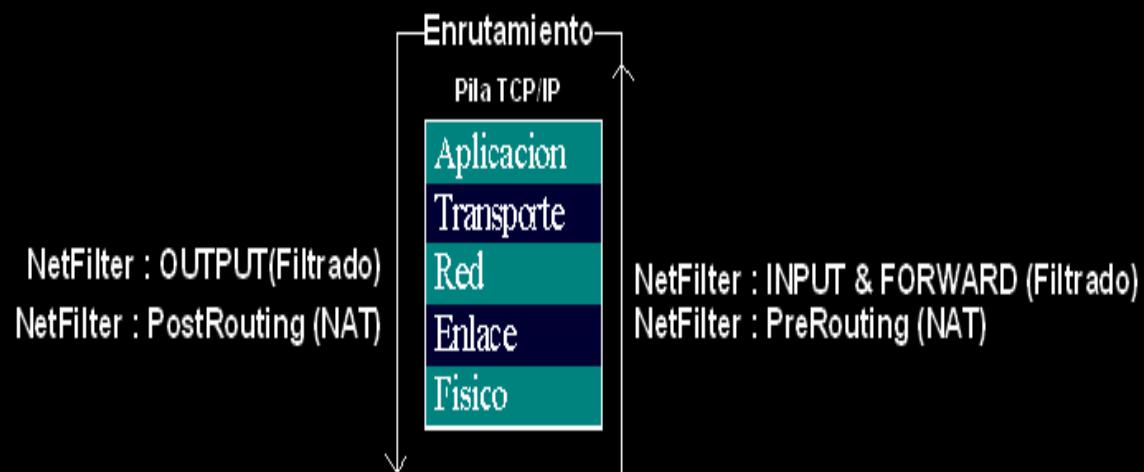
```
# DNAT de ip real (VIRTUAL) hacia Vulcano, con el puerto 21
iptables -t nat -A PREROUTING -d $VIRTUAL -j DNAT -p tcp --dport
21 --to $VULCANO      # FTP

# SNAT de Caligula con la ip VIRTUAL
iptables -t nat -A POSTROUTING -o eth0 -s $CALIGULA      -j SNAT
--to $VIRTUAL

#HTTP Proxy transparente a traves de SQUID en VULCANO
iptables -t nat -A PREROUTING -d ! $LOCALNET -s $PRIVATE -p tcp
--dport 80 -j DNAT --to $VULCANO:8080
```

Implementación. NAT XI

- ¿Cuál es el orden de aplicación del filtrado y el NAT ?

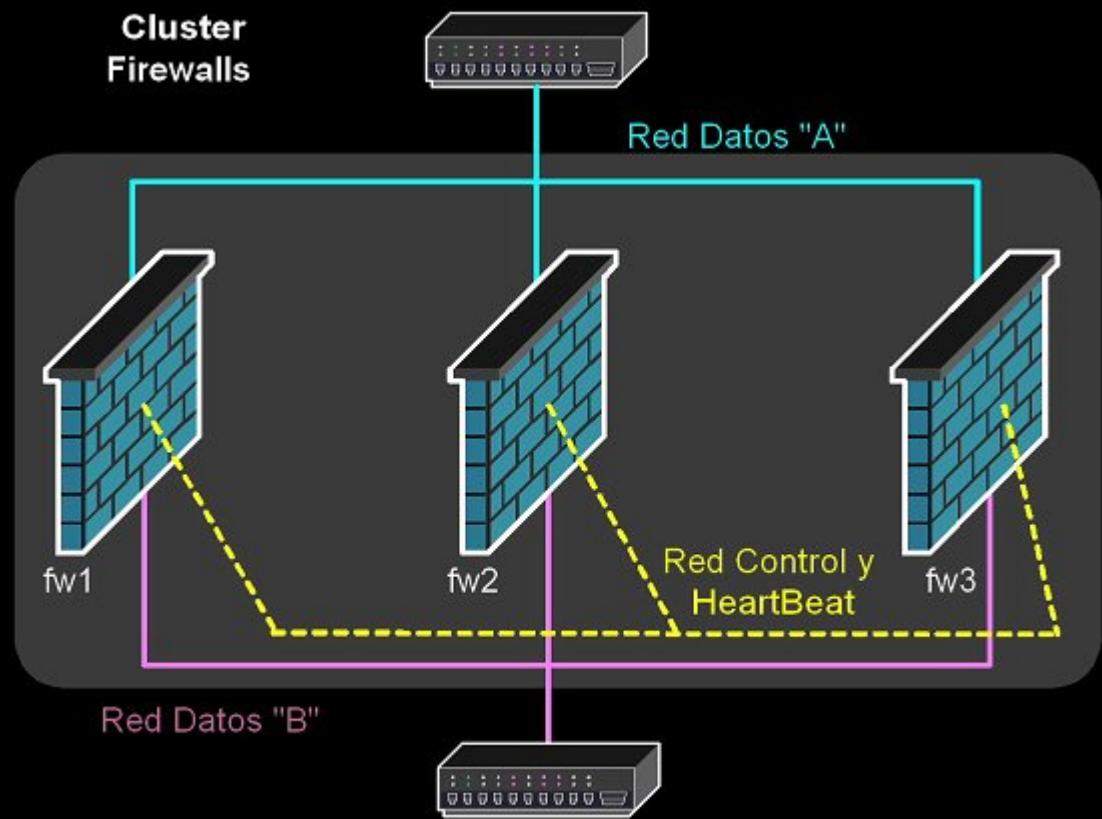


HA en Firewalls

- Conceptos de HA
- Tipos de HA
 - ◆ Clustering
 - ◆ HA Hot Standby (pasivo/activo)
 - ◆ HA Activo/Activo
 - ◆ HA A/A con Load Sharing.

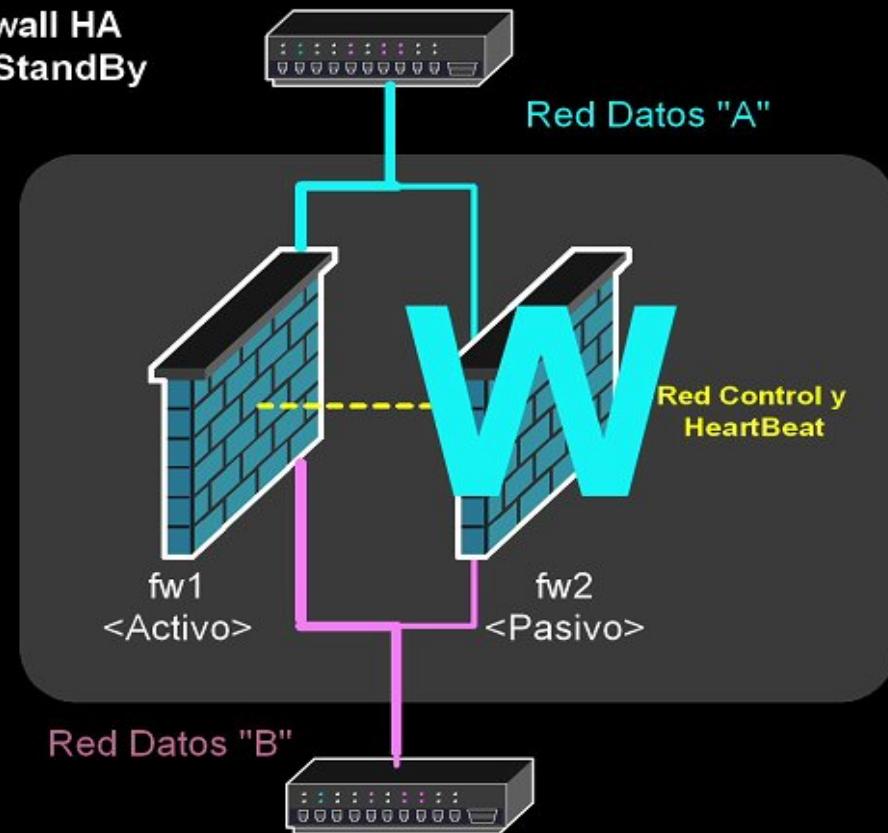
HA en Firewalls I

- Clustering



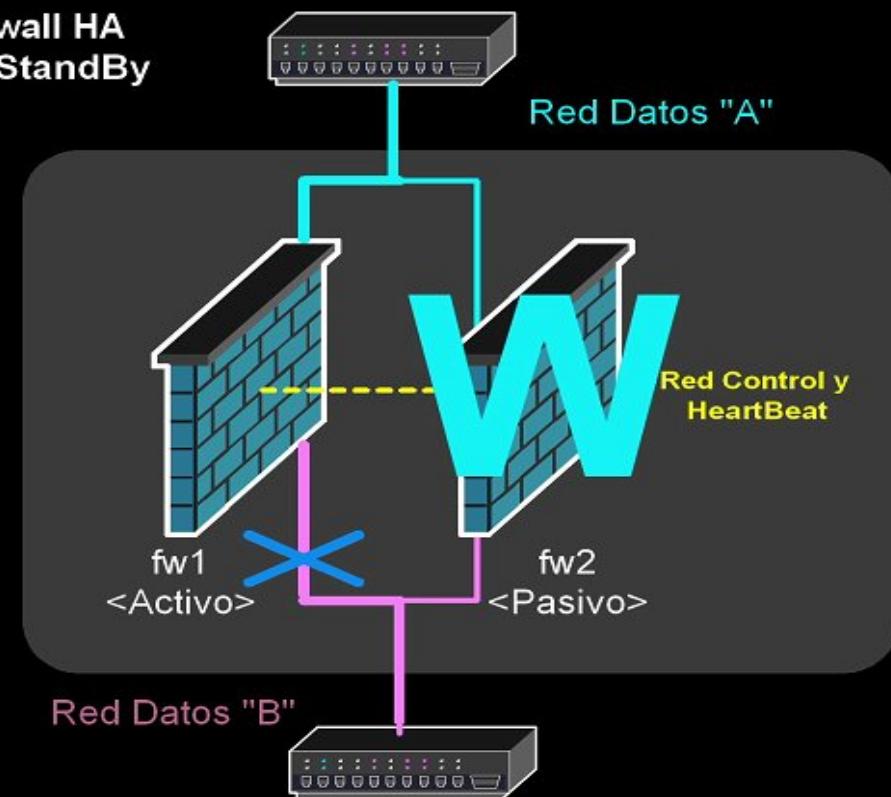
HA en Firewalls II

- HA Hot StandBy Activo/Pasico



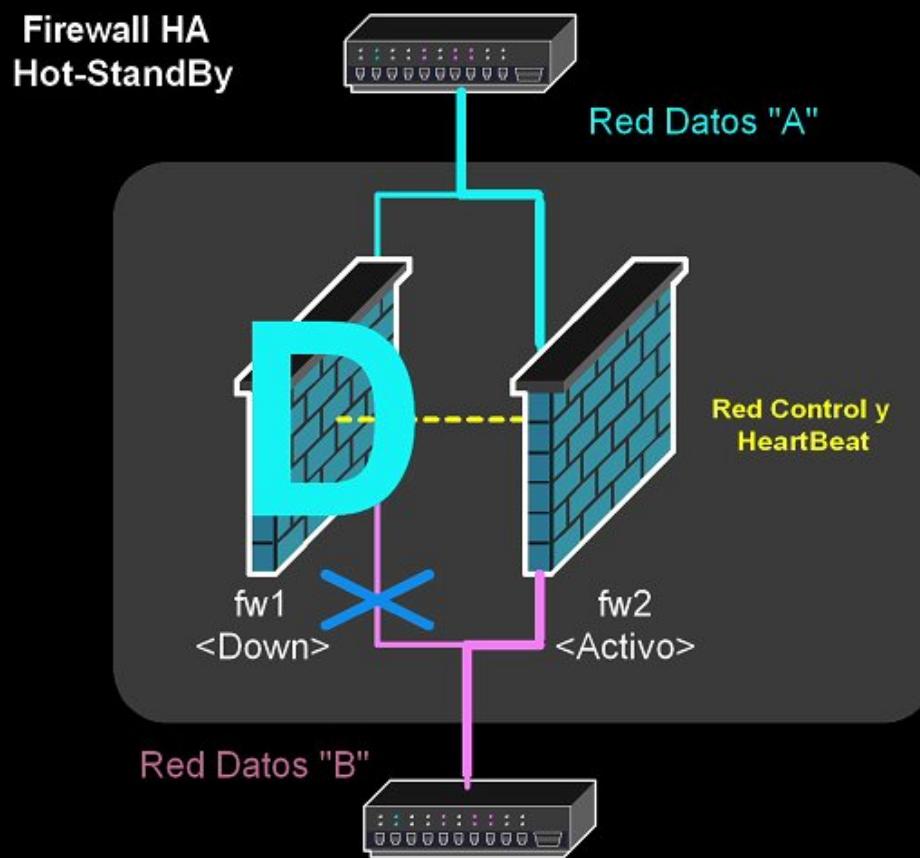
HA en Firewalls III

- Hot StandBy, fallo



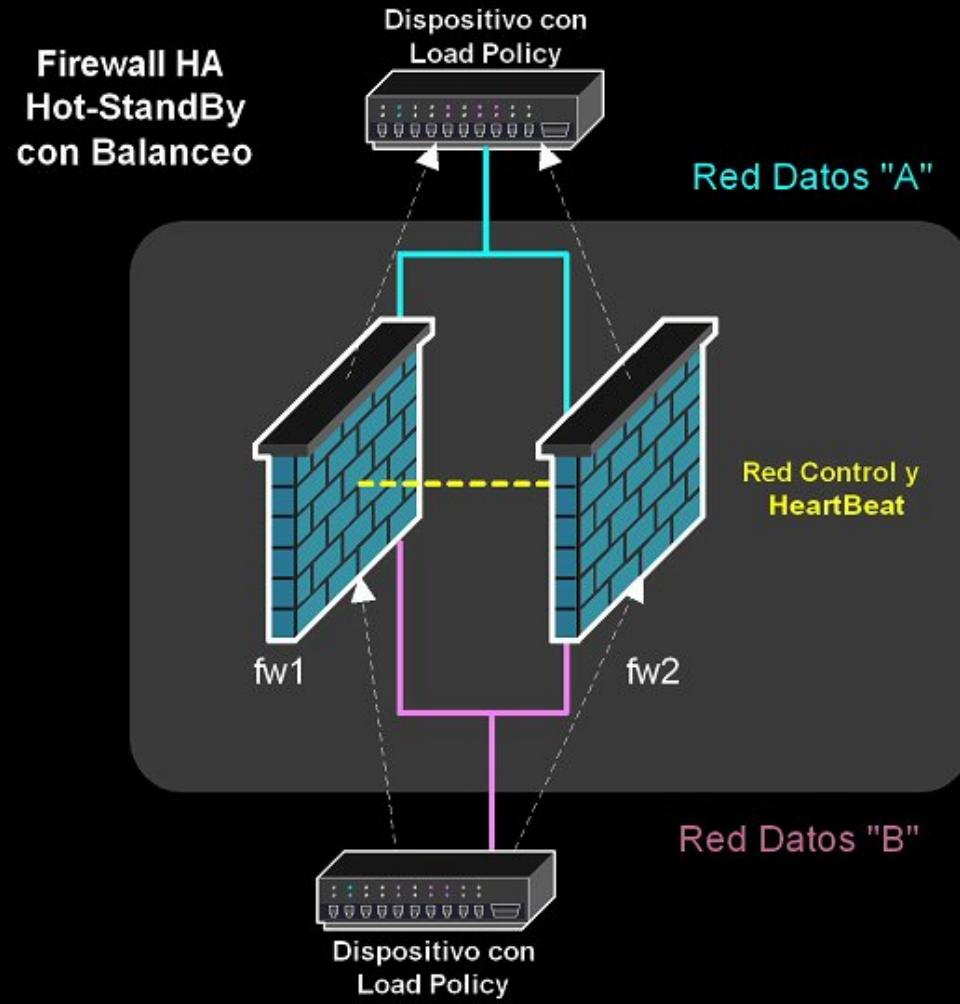
HA en Firewalls IV

- Hot StandBy, switch over



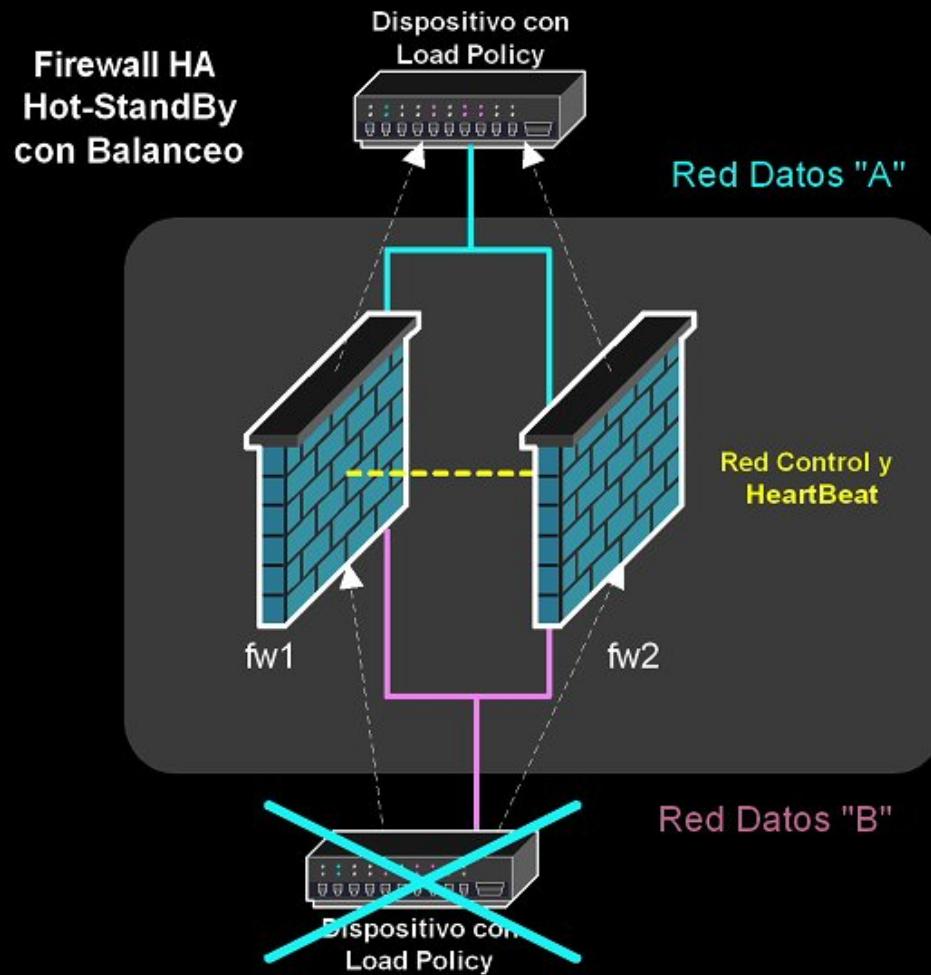
HA en Firewalls V

- HA Activo/Activo: Load Sharing



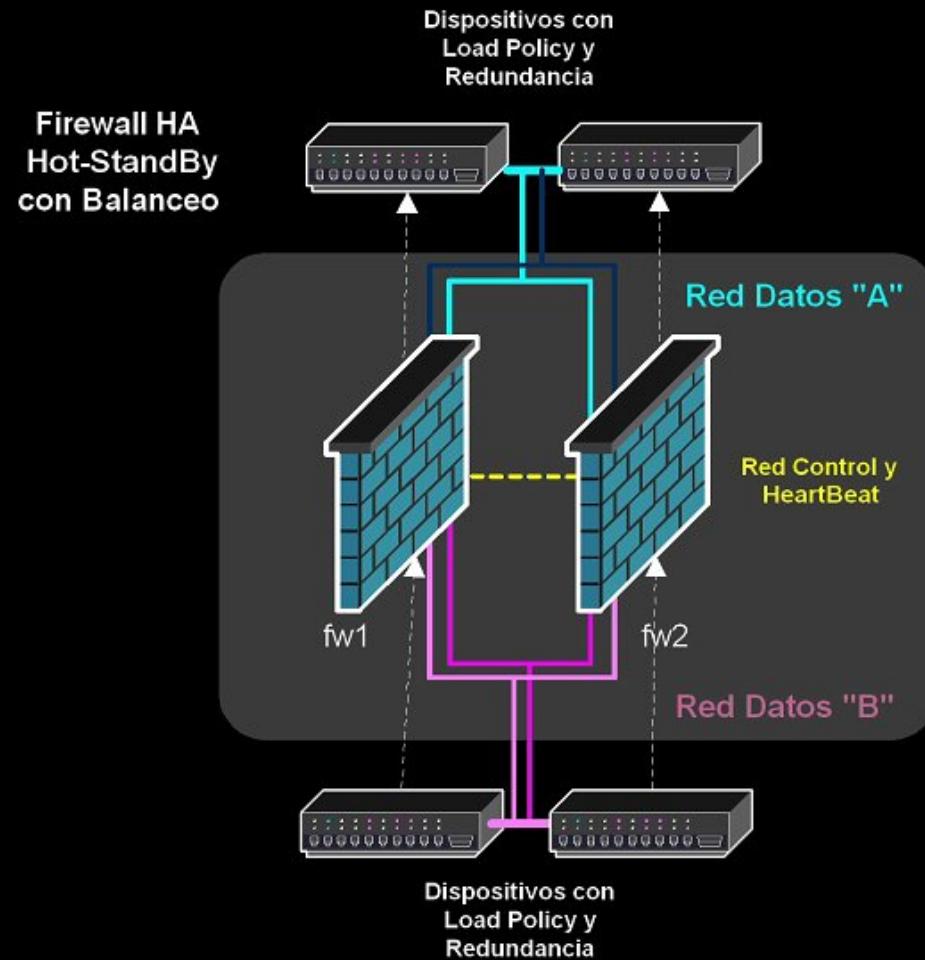
HA en Firewalls VI

- ¿Es esto perfecto?.



HA en Firewalls VII

■ HA Integral y Load Sharing



Implementando HA

- VRRP. Rfc 2338
 - ◆ Cisco HSRP
 - ◆ Autenticación
- Standard y fabricantes.
 - ◆ Firewalls
 - ◆ Electronica de red
 - ◆ SSOO

Implementando VRRP I

■ Arranque

```
#!/bin/bash
#
# VRRP Daemon Start, 01/03/02
# Sancho Lerena, slerena@gnusec.com

LISTA_PROCESOS=`ps -A | grep "vrrpd" | tr -s " " | cut -d " " -f 2`
if [ -n "$LISTA_PROCESOS" ]
then
    echo " There are present VRRP daemons running. Aborting."
else
    echo "Arrancando demonio VRRP en eth1/192.168.5/24"
    nohup vrrpd -v 105 -p 100 -i eth1 192.168.5.100 > /dev/null &
    echo "Arrancando demonio VRRP en eth0/192.168.6/24"
    nohup vrrpd -v 106 -p 100 -i eth0 192.168.6.100 > /dev/null &
    echo "Waiting for VRRP Daemons"
    sleep 10
    echo "Restoring IP routing"
    route add default gw 192.168.5.1; fi;
```

Implementando VRRP II

■ Parada

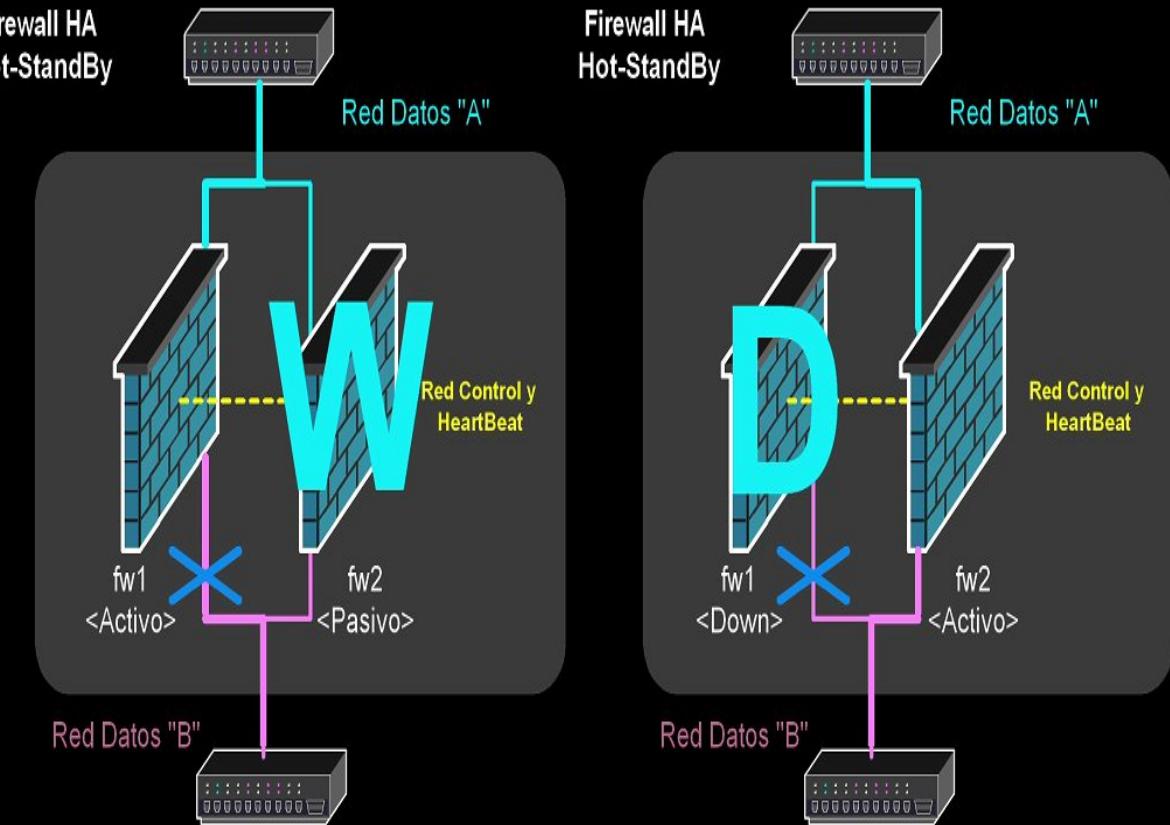
```
#!/bin/bash
# VRRP Daemon Stop, 01/03/02
# Sancho Lerena, slerena@gnusec.com

if [ "$1" == "-?" ]
then
    echo "Syntax:"
    echo "      vrrp-stop [-f] "
    echo " "
    echo " -f : force kill with signal 9 "
    exit
fi;

# Obtener el PID de los procesos en memoria
LISTA_PROCESOS=`ps -A | grep "vrrpd" | tr -s " " | cut -d " " -f 2`
if [ -z "$LISTA_PROCESOS" ]
then
    echo " No VRRP Daemons present. Aborting."
else
    echo " Killing all VRRP daemons"
    if [ "$1" == "-f" ]
    then
        kill -s 9 $LISTA_PROCESOS
    else
        kill $LISTA_PROCESOS
    fi;
fi;
```

Implementando VRRP III

- Monitorización.
 - ◆ Problema del agujero negro



Implementando VRRP IV

■ Monitorización

```
#!/bin/bash

# Checking conectivity with ICMP Ping, VRRPD Companion Script
VER="11/03/2002 - v1.0"

SLEEP_TIME=$2           # Tiempo de parada entre checks, en segundos
if [ -z $2 ]
then
    SLEEP_TIME=5       # Si no se especifica, el check es cada 5 segundos
fi;

# Obtener el PID de los procesos de VRRPD en memoria
LISTA_PROCESOS=`ps -A | grep "vrrpd" | tr -s " " | cut -d " " -f 2`
if [ -z "$LISTA_PROCESOS" ]
then
    echo " No VRRP Daemon running, aborting. "
    exit
fi;

IP_DESTINO=$1          # IP de comprobacion, pasada como 1# parametro
COMANDO=`ping -c 1 "$IP_DESTINO" | grep '100% packet loss'`"
RES=0

while [ "$RES" -eq 0 ];do
    if [ ! -z "$COMANDO" ] ;then
        echo " Ping fail "
        echo " Shutting down VRRP daemons "
        kill -s 9 $LISTA_PROCESOS
        RES=1;else
        echo " Debug: Ping ok"
        sleep $SLEEP_TIME
    fi;done;
```

Detectores de intrusión

- Fundamentos de un IDS
- Tipos
 - ◆ Host / Servidor / FS
 - ◆ Red
- Arquitecturas distribuidas
- Importancia de las actualizaciones

IDS. Snort

- Que es SNORT
- Plataformas y rendimiento
- Arquitectura
 - ◆ Configuracion
 - ◆ Filtros
 - ◆ Reglas
 - ★ Actualización
- Respuestas activas
- Manejo de incidencias
 - ◆ SnortSnarf
 - ◆ SQL

Implementando Snort I

■ Informes automatizados

SILICON DEFENSE **SnortSnarf start page**

All Snort signatures

SnortSnarf v010821.1

4193 alerts found using input module SnortFileInput, with sources:

- /var/log/snort/snort.alert

Earliest alert at **06:30:58.150805** on **03/11/2002**
Latest alert at **06:29:56.611588** on **03/12/2002**

Signature (click for sig info)	# Alerts	# Sources	# Destinations	Detail link
MISC Large ICMP Packet [arachNIDS]	1074	58	8	Summary
SCAN nmap TCP [arachNIDS]	978	17	5	Summary
INFO MSN chat access	915	1	39	Summary
SNMP request udp [CVE]	460	1	1	Summary
SHELLCODE x86 inc ebx NOOP	277	31	1	Summary
INFO ICQ access	229	1	18	Summary
SNMP public access udp [CVE]	92	1	1	Summary
EXPERIMENTAL SHELLCODE x86 NOOP	70	22	2	Summary
DDOS shaft client to handler [arachNIDS]	55	6	1	Summary
SHELLCODE x86 NOOP [arachNIDS]	19	6	1	Summary
SHELLCODE x86 setuid 0 [arachNIDS]	6	3	1	Summary
ICMP Source Quench (Undefined Code!)	4	3	4	Summary

Implementando Snort II

■ Investigando ataques

SILICON DEFENSE **SnortSnarf signature page**

DNS SPOOF query response with ttl: 1 min. and no authority

SnortSnarf v010821.1

1 alerts with this signature using input module SnortFileInput, with sources:

- /var/log/snort/snort.alert

Earliest such alert at **02:38:30.018070** on **03/12/2002**
Latest such alert at **02:38:30.018070** on **03/12/2002**

DNS SPOOF query response with ttl: 1 min. and no authority	1 sources	1 destinations
Rules with message "DNS SPOOF query response with ttl: 1 min. and no authority".		
alert udp \$EXTERNAL_NET 53 -> \$HOME_NET any (msg:"DNS SPOOF query response with ttl: 1 min. and no authority"; content:"\$1 80 00 01 00 01 00 00 00 00"; content:" e0 0c 00 01 00 01 00 00 3c 00 04 "; classtype:bad-unknown; sid:254; rev:2;) (from <i>dns.rules</i>)		

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
[REDACTED]	1	1	1	1

Implementando Snort III

■ Investigando atacantes

The screenshot shows a web-based interface for analyzing Snort alerts. At the top, there's a logo for "SILICON DEFENSE" featuring two eyes. The main title is "SnortSnarf alert page" and the source IP listed is "Source: 217.126.145.185". Below this, it says "SnortSnarf v010821.1". A message indicates "2 such alerts found using input module SnortFileInput, with sources:". A bullet point lists the source as "/var/log/snort/snort.alert". Below this, it shows the earliest and latest timestamps of the alerts. It also notes that there are 1 different signatures present for the source IP. A bullet point lists "2 instances of INFO VNC server response". Finally, it states that there are 1 distinct destination IPs in the alerts of the type on this page.

SILICON DEFENSE

SnortSnarf alert page

Source: 217.126.145.185

SnortSnarf v010821.1

2 such alerts found using input module SnortFileInput, with sources:

- /var/log/snort/snort.alert

Earliest: 11:47:22.055772 on 03/11/2002
Latest: 15:55:40.528649 on 03/11/2002

1 different signatures are present for 217.126.145.185 as a source

- 2 instances of INFO VNC server response

There are 1 distinct destination IPs in the alerts of the type on this page.

217.126.145.185	Whois lookup at:	ARIN	RIPE	APNIC	Geektools
	DNS lookup at:	Amenesi	TRIUMF	Princeton	

03/11-11:47:22.055772 [**] [1:560:2] INFO VNC server response [**] [Classification: Misc activity] [Priority: 3] (TCP) 217.126.145.185:5900 -> 217.126.145.185:5900

Gestión y Monitorización

- Importancia de la gestión y la monitorización
 - ◆ Analizadores de tráfico
 - ◆ Gestores SNMP
 - ◆ Gestores QoS
 - ◆ Otras herramientas

Analizadores de tráfico

- Analizadores de tráfico
 - ◆ IPTraf
 - ◆ NTOP
 - ◆ tcpdump ☺

Analizadores. IPTraf I

■ Iptraf. Estadísticas real-time

IPTraf						
Statistics for eth1 -						
	Total Packets	Total Bytes	Incoming Packets	Incoming Bytes	Outgoing Packets	Outgoing Bytes
Total:	21225	10179566	21225	10179566	0	0
IP:	21223	9836212	21223	9836212	0	0
TCP:	20663	9794868	20663	9794868	0	0
UDP:	136	17168	136	17168	0	0
ICMP:	341	20856	341	20856	0	0
Other IP:	83	3320	83	3320	0	0
Non-IP:	2	686	2	686	0	0
Total rates:		254.6 kbytes/sec	Broadcast packets:		0	
		507.0 packets/sec	Broadcast bytes:		0	
Incoming rates:		254.6 kbytes/sec	IP checksum errors:		0	
		507.0 packets/sec				
Outgoing rates:		0.0 kbytes/sec				
		0.0 packets/sec				

Analizadores. IPTraf III

■ Iptraf. Sesiones TCP/UDP

```
IPTraf
TCP Connections <Source Host:Port>
[10.16.15.60:telnet
[10.16.11.22:3017
[10.16.11.11:1131
[205.164.12.77:46864
[63.254.17.61:www
[10.16.14.99:1946
[10.16.1.200:3014
[232.11.3.25:https
[12.67.49.5190
[11.128.14.41:1140
[11.128.11.11:1188
[10.16.130.52:telnet
[10.128.1.200:1177
[64.12.27.86:5190
[63.236.18.52:www
[10.128.1.194:4542
[11.128.1.27:1148
[64.11.9.47:5190
[64.12.25.0:5190
[10.17.11.122:2375
[10.16.130.62:34201
[10.128.11.22:x11
[10.1.8.1.20:1144
[64.12.27.53:5190
[5.128.11.248:4949
[10.1.130.52:telnet
[10.128.1.08:1871
[64.12.192.1863
[64.12.15.4:5190
TCP: 194 entries
          Packets      Bytes   Flags   Iface
          >    71       61205  -PA-   eth1
          >    63        2520   --A-   eth1
          >   266       14396  --A-   eth1
          >   476       701136  --A-   eth1
          >   40        34460  -PA-   eth1
          >   39        1560   --A-   eth1
          >   2         910   -PA-   eth1
          >   2        151   --A-   eth1
          >   1         40   --A-   eth1
          =   0         0   ----   eth1
          >   10        400   --A-   eth1
          >   16       19923  -PA-   eth1
          >   1         46   -PA-   eth1
          =   0         0   ----   eth1
          =   10       12088  --A-   eth1
          =   7        585   --A-   eth1
          >   1         46   -PA-   eth1
          =   0         0   ----   eth1
          >   1         40   --A-   eth1
          >   1         46   -PA-   eth1
          >   1         46   -PA-   eth1
          >   1         46   -PA-   eth1
          >   301      326884  -PA-   eth1
          >   164      6560   --A-   eth1
          >   1         46   -PA-   eth1
          =   0         0   ----   eth1
          >   10        520   --A-   eth1
          >   16       20115  -PA-   eth1
          >   5         200   --A-   eth1
          >   4         753   -PA-   eth1
          >   37      23700  --A-   eth1
          Active
          UDP (76 bytes) From 10.128.1.120:3937 to 10.16.11.1131:52ntp on eth1
          UDP (76 bytes) From 10.128.120.52:ntp to 10.16.11.1131:3937 on eth1
          UDP (383 bytes) From 10.128.17.2:netbios-ns to 10.128.11.152:netbios-ns on eth1
          IP protocol 112 (40 bytes) From 10.128.11.22 to 224.0.0.18 on eth1
          IP protocol 112 (40 bytes) From 10.128.11.22 to 224.0.0.18 on eth1
          UDP (383 bytes) From 10.128.65.2:netbios-ns to 10.128.11.101.152:netbios-ns on eth1
          UDP (62 bytes) From 10.128.17.7:4433 to 10.128.11.101:domain on eth1
          UDP (56 bytes) From 10.128.11.105:3267 to 10.128.11.0.49:domain on eth1
          UDP (134 bytes) From 192.13.0.49:domain to 10.128.11.105:3267 on eth1
          UDP (56 bytes) From 10.128.11.105:3267 to 10.128.11.1.2:domain on eth1
          UDP (150 bytes) From 10.128.11.1.2:domain to 10.128.11.105:3267 on eth1
          UDP (172 bytes) From 10.128.11.10.10:domain to 10.128.11.65.3:4433 on eth1
          UDP (67 bytes) From 10.128.11.207.12:domain to 10.128.11.12:domain on eth1
          UDP (65 bytes) From 10.128.11.43:4089 to 10.128.11.128.27:domain on eth1
          UDP (65 bytes) From 10.128.11.105:1552 to 10.128.11.93.92.5:domain on eth1
          UDP (59 bytes) From 10.128.11.105:3267 to 10.128.11.4.0.49:domain on eth1
          Bottom -- Elapsed time: 0:00:00
          IP: 2043645   TCP: 2036600   UDP: 6045   ICMP: 40   Non-IP: 0
          Up/Dn/PgUp/PgDn-scroll  M-more TCP info  W-chg actv win  S-sort TCP  X-exit
```

Analizadores. NTOP

- Importancia del análisis de red
 - ◆ Errores
 - ◆ Malos usos
 - ◆ Control de la red
 - ★ Hosts desconocidos
 - ★ Trafico
 - ★ Control de Carga

Implementando NTOP I

■ Informacion global

Global Traffic Statistics

Nw Interface Type	eth1 (Ethernet) [0.0.0.0/255.255.255.255]	
Sampling Since	Mon Mar 11 13:29:03 2002 [1 day(s) 5:49:56]	
Total	23,454,865	
Dropped by the kernel	0	
Dropped by ntop	0	
Unicast	99.1%	23,243,902
Broadcast	0.0%	703
Multicast	0.9%	210,260

Multicast
Broadcast
Unicast

Packets

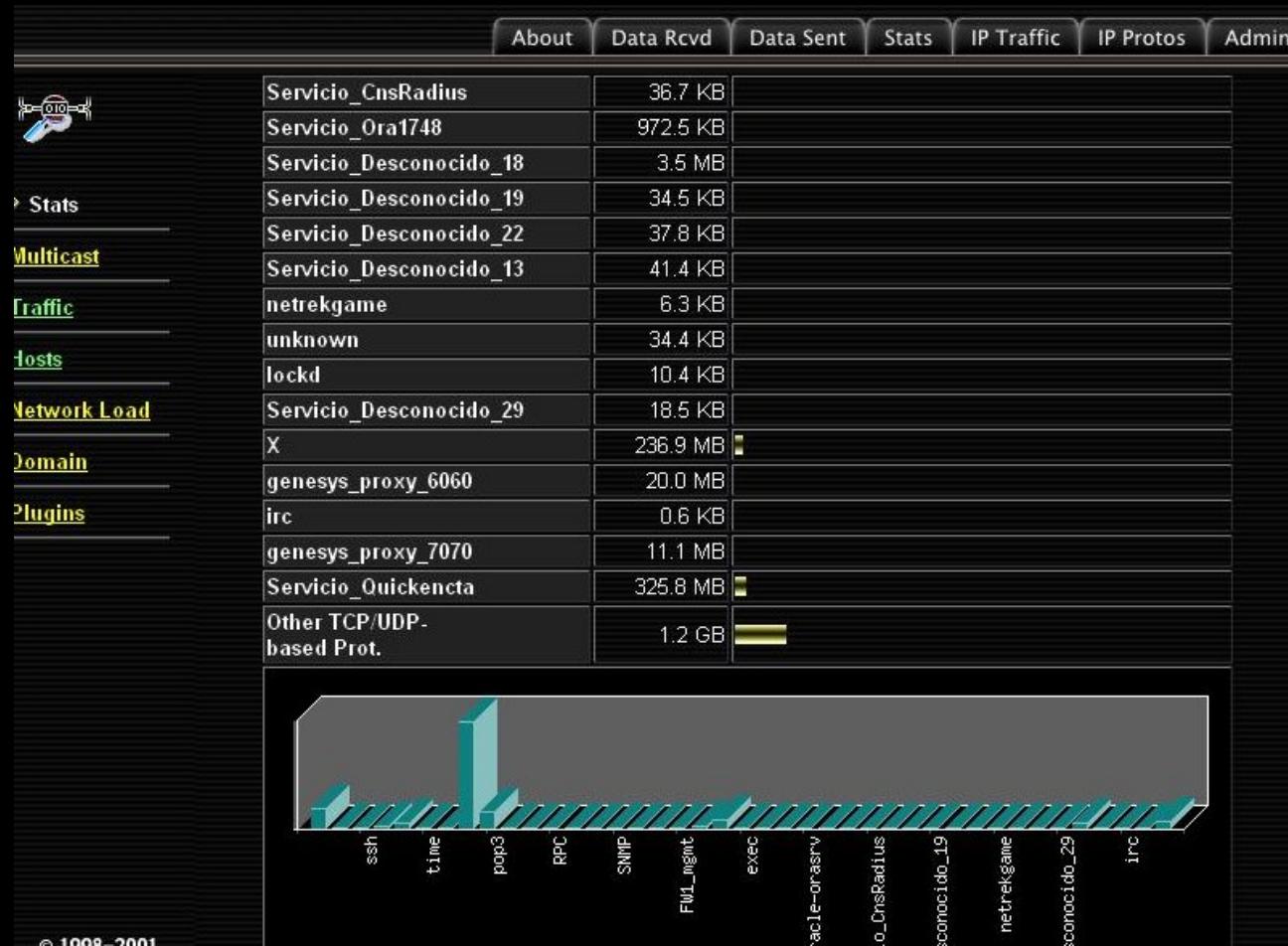
Shortest	60 bytes
Average Size	596 bytes
Longest	1,514 bytes
< 64 bytes	44.5% 10,429,081
< 128 bytes	16.2% 3,804,516
< 256 bytes	9.4% 2,207,388
< 512 bytes	5.7% 1,325,668
< 1024 bytes	2.4% 4,555,720

About Data Rcvd Data Sent Stats IP Traffic IP Protos Admin

© 1998-2001 by Luca Deri

Implementando Ntop II

- Informacion de tráfico TCP/UDP



Implementando NTOP III

- Informacion de cada host

		About	Data Rcvd	Data Sent	Stats	IP Traffic	IP Protos	Admin
Load	IP Address	216.52.146.227 [unicast]						
	First/Last Seen	03/12/02 19:04:40 - 03/12/02 19:04:40 [0 sec]						
	Last MAC Address/Router	00:00:5E:00:01:04						
	Host Location	Remote (outside specified/local subnet)						
	IP TTL (Time to Live)	125:234 hops						
	Total Data Sent	158/1 Pkts/0 Retran. Pkts [0%]						
	Broadcast Pkts Sent	0 Pkts						
	Data Sent Stats	Remote (100 %)						
	Total Data Rcvd	77/1 Pkts/0 Retran. Pkts [0%]						
	Data Received Stats	Remote (100 %)						
Provided Services	 Name Server							
Host Physical Location								

Implementando Ntop IV

- Informacion detallada de sesiones

The screenshot displays the Ntop IV web-based interface with the following sections:

- Last Contacted Peers:** A table showing recent peer contacts. The columns are: Receiver Name, Receiver Address, Sender Name, and Sender Address. The data is heavily redacted.
- IP Service Stats: Client Role:** A table showing statistics for the HTTP service. The columns are: IP Service, # Loc. Req. Sent, # Rem. Req. Sent, # Pos. Reply Rcvd, # Neg. Reply Rcvd, Local RndTrip, and Remote RndTrip. The data is heavily redacted.
- TCP/UDP Service/Port Usage:** A table showing port usage for various services. The columns are: IP Service, Port, # Client Sess., Last Client Peer, # Server Sess., and Last Server Peer. The data is heavily redacted.

Implementando Ntop V

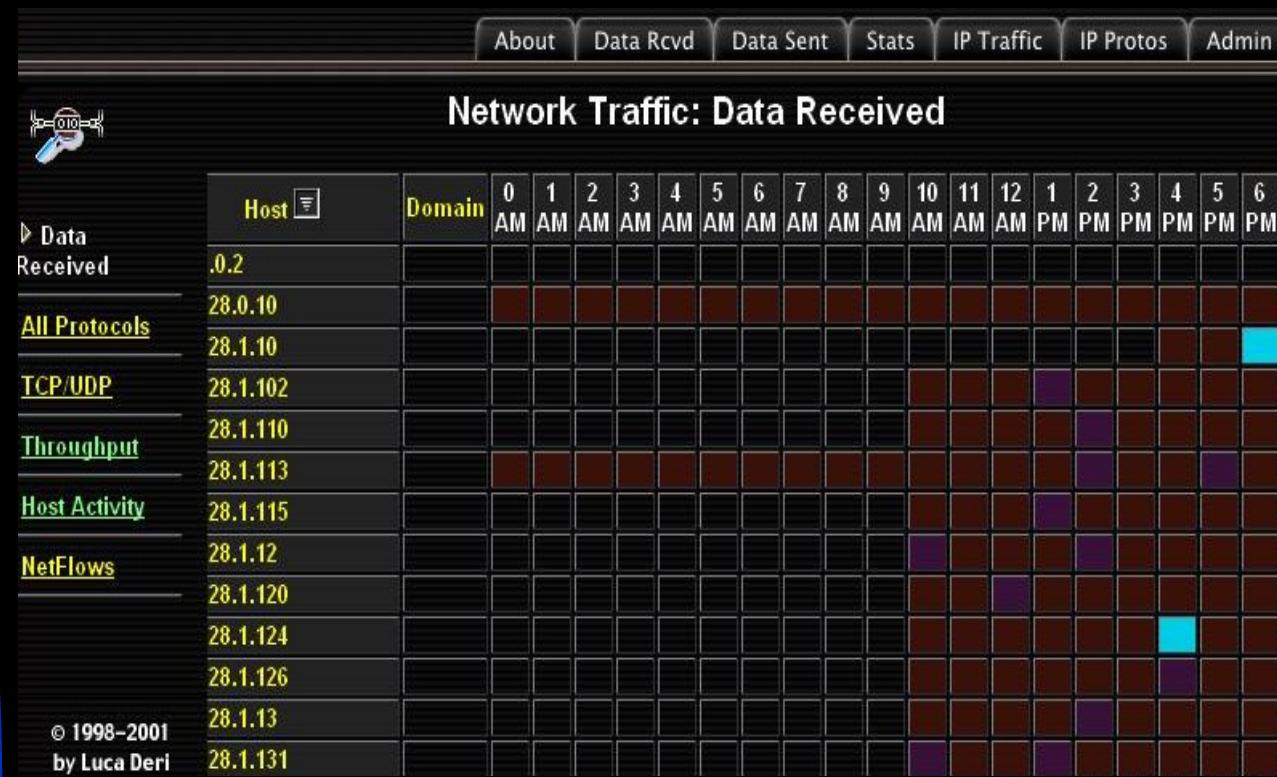
- Informacion general de hosts

The screenshot shows the 'Network Traffic: Data Received' section of the Ntop interface. The table lists various hosts along with their domain, actual throughput, average throughput, peak throughput, and packet throughput statistics.

	Host	Domain	Actual Thpt	Avg Thpt	Peak Thpt	Actual Pkt Thpt	Avg Pkt
Data Received	192.168.1.11		191.9 Kbps	64.2 Kbps	1.1 Mbps	146.6 Pkts/sec	47.3 Pkt
All Protocols	192.168.1.194		151.5 Kbps	2.0 Kbps	389.6 Kbps	30.3 Pkts/sec	0.7 Pkt
CP/UDP	192.168.1.103		136.5 Kbps	8.5 Kbps	217.4 Kbps	11.7 Pkts/sec	0.8 Pkt
Throughput	192.168.1.312		125.3 Kbps	4.8 Kbps	1.1 Mbps	17.0 Pkts/sec	1.9 Pkt
Host Activity	192.168.1.248		122.2 Kbps	15.7 Kbps	1.4 Mbps	20.8 Pkts/sec	2.7 Pkt
NetFlows	192.168.1.11		89.1 Kbps	6.1 Kbps	657.0 Kbps	8.3 Pkts/sec	1.5 Pkt
	192.168.1.17		88.1 Kbps	1.6 Kbps	498.2 Kbps	43.8 Pkts/sec	0.7 Pkt
	192.168.1.122		84.6 Kbps	4.1 Kbps	448.0 Kbps	7.8 Pkts/sec	1.0 Pkt
	192.168.1.64		62.7 Kbps	4.4 Kbps	1.3 Mbps	11.0 Pkts/sec	0.7 Pkt
	192.168.1.121		60.7 Kbps	9.6 Kbps	192.4 Kbps	17.4 Pkts/sec	4.2 Pkt
	192.168.1.31		46.1 Kbps	2.3 Kbps	333.3 Kbps	4.8 Pkts/sec	0.3 Pkt
	192.168.1.42		41.8 Kbps	7.5 Kbps	978.8 Kbps	11.1 Pkts/sec	2.0 Pkt
	192.168.1.42		37.9 Kbps	1.3 Kbps	173.4 Kbps	4.8 Pkts/sec	0.2 Pkt
	192.168.1.71		36.5 Kbps	369.9 bps	63.2 Kbps	5.0 Pkts/sec	0.1 Pkt
	192.168.1.112		36.1 Kbps	1.0 Kbps	43.3 Kbps	12.4 Pkts/sec	0.3 Pkt
	192.168.1.60		30.1 Kbps	455.2 bps	55.8 Kbps	11.1 Pkts/sec	0.1 Pkt
	192.168.1.66		22.8 Kbps	5.2 Kbps	139.4 Kbps	3.0 Pkts/sec	0.8 Pkt
	192.168.1.231		21.1 Kbps	334.9 bps	74.5 Kbps	2.2 Pkts/sec	0.1 Pkt
	192.168.1.22		20.1 Kbps	768.2 bps	100.5 Kbps	3.2 Pkts/sec	0.3 Pkt
	192.168.1.102		19.9 Kbps	862.7 bps	189.5 Kbps	2.0 Pkts/sec	0.2 Pkt
	192.168.1.162.89		19.7 Kbps	539.4 bps	19.7 Kbps	15.1 Pkts/sec	0.4 Pkt
	192.168.1.208		15.0 Kbps	520.2 bps	83.9 Kbps	1.7 Pkts/sec	0.2 Pkt

Implementando Ntop VI

- Monitorizacion continua de red, con historicos y logs.



Implementando NTOP VII

- Definición de flujos de usuario

Network Flows

Flow Name	Packets	Traffic
FTP_To_CPD	132,234	7.8 MB
WEB_To_CPD	1,350,084	198.4 MB
eDonkey2000	4,466	2.0 MB
FastTrack	6,149	2.1 MB
icmpWatchPlugin	0	0

Throughput

Report created on Tue Mar 12 19:29:23 2002 [1 day(s) 6:00:20]
Generated by **ntop** v.2.0.0 MT [i686-pc-linux-gnu] (10/30/01 10:10:24 AM build)
listening on 
© 1998-2001 by L. Deri

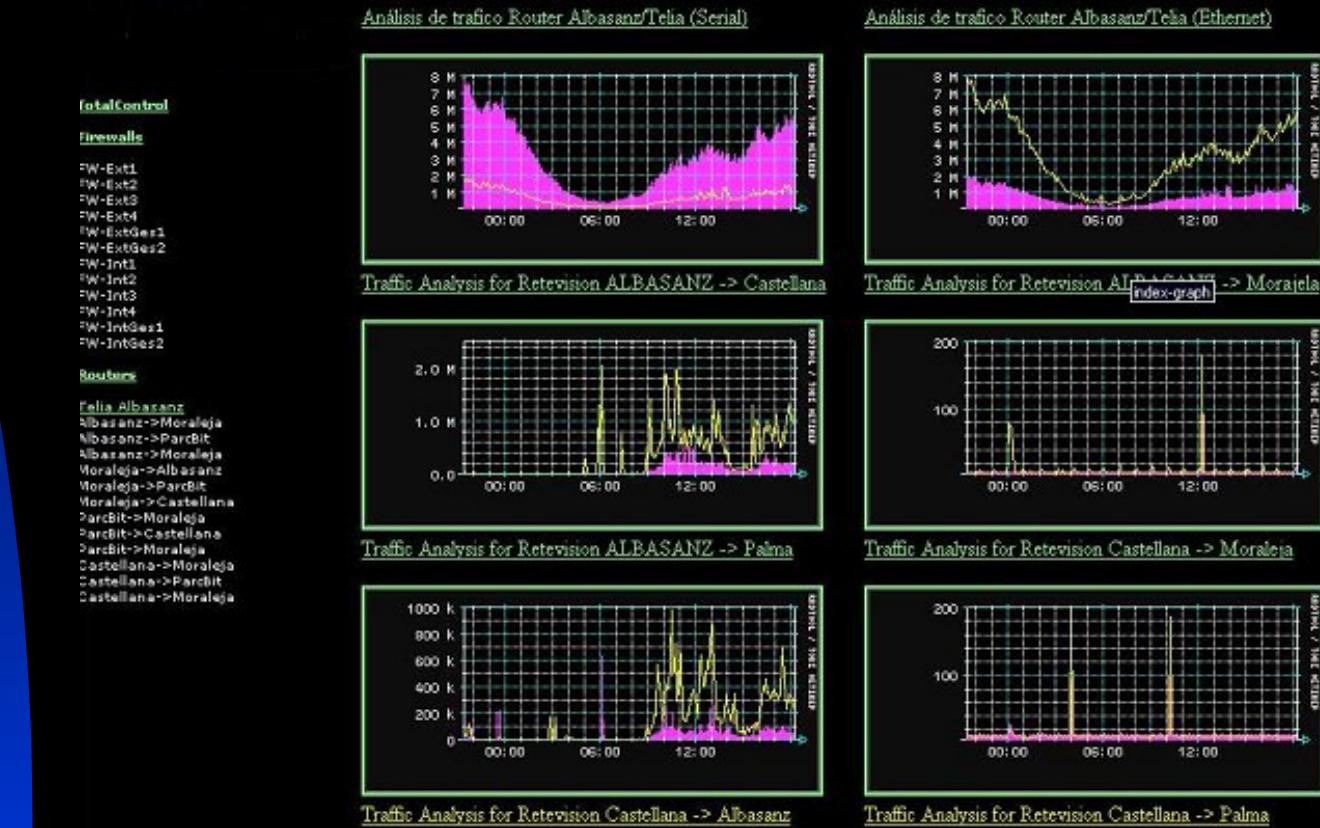
© 1998-2001

Gestión y monitorización

- SNMP
- Herramientas
 - Netsaint
 - MRTG/RRD

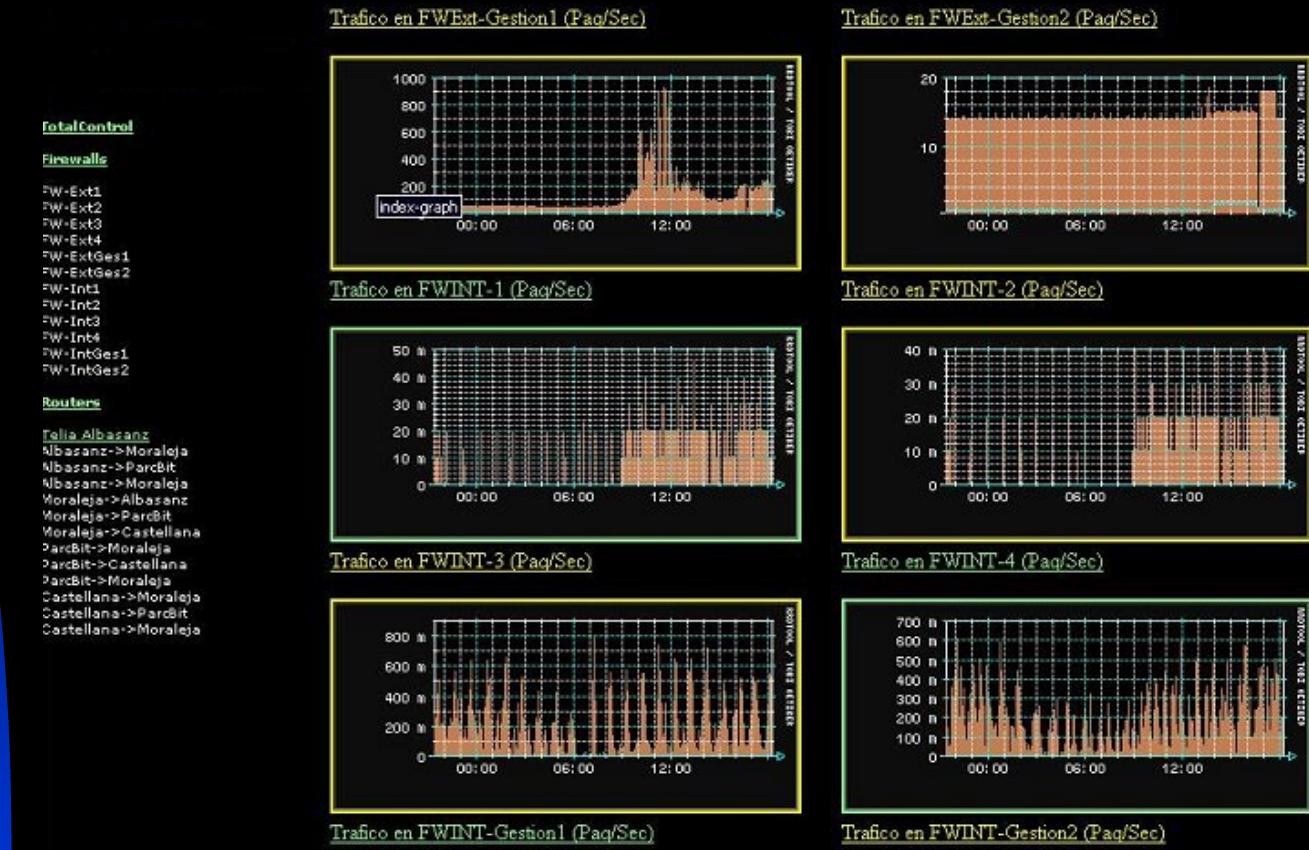
Gestion SNMP. MRTG I

■ Carga de red



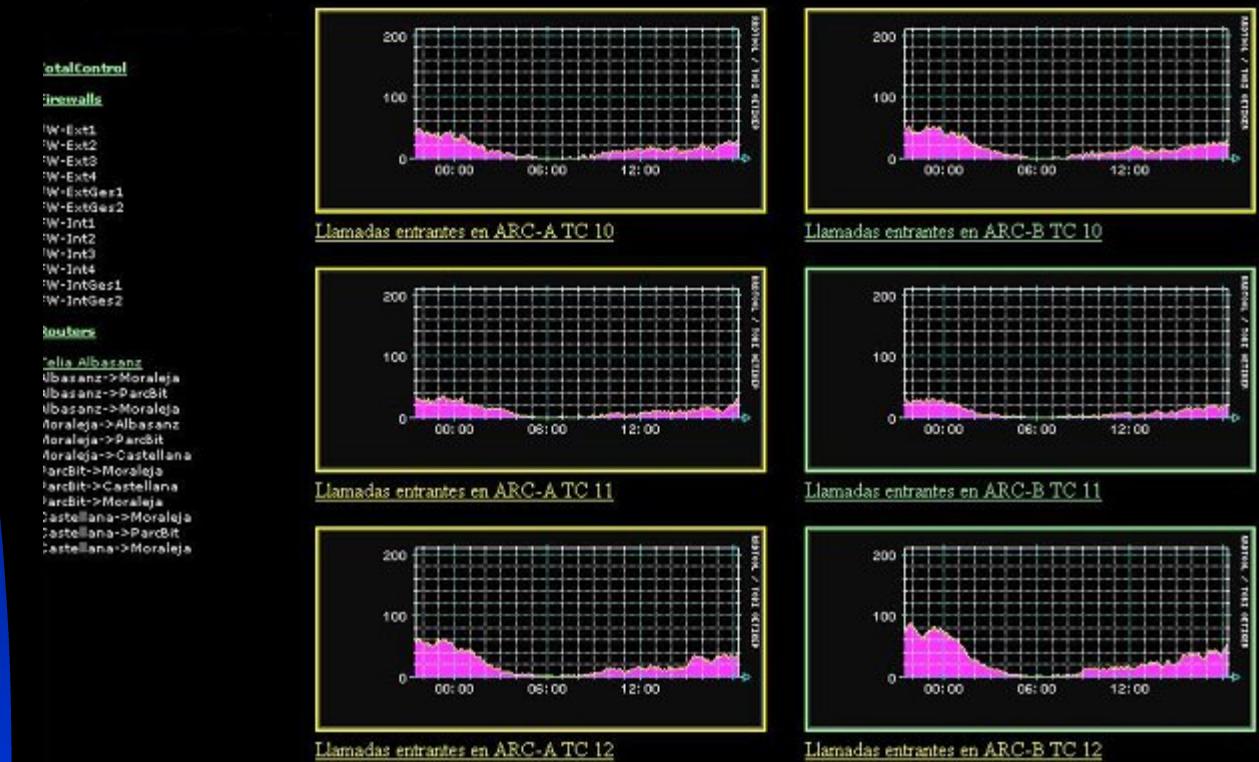
Gestion SNMP. MRTG II

■ Carga de firewalls



Gestion SNMP. MRTG III

- Carga de llamadas en un RAS



Parte III - Tema D

Auditoría en GNU/Linux



Auditoría GNU

- Introducción
- NESSUS
- Otras herramientas

Parte IV

Respuesta ante incidentes

Parte V

Recursos