Seguridad y Sistemas en IPv6

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
MINISTERIO DE CIENCIA E INNOVACIÓN

IPv6 : Dispositivo

Cortafuegos y/o filtros

- La mayoria de los fabricantes soportan IPv6, aunque:
  - Pueden necesitar actualizaciones de hardware/licencias
  - No tengan todas las funcionalidades de IPv4

IDS/NIDS:

- Snort: Soporte IPv6 desde 2.8.0
- Pocas reglas específicas de IPv6

Inspectores de contenido: ¿?

Balanceadores de tráfico:

- F5, alteon: soporte IPv6

IPv6: Cabeceras y filtrado:

En IPv4 el tipo de protocolo va incluido dentro de la cabecera IP.

La posición del puerto (origen/ destino) es fija dentro de la cabecera TCP)

Facil de procesar “en hardware”

En IPv6 la información sobre el protocolo no va incluida en la cabecera IPv6, sino en otra cabecera propia.

Puede haber otras cabeceras de opciones antes del la cabecera TCP/UDP

Más caro de procesar “en hardware”

IPv6: Tuneles:

Posibilidad de accesos desde el exterior no deseados.

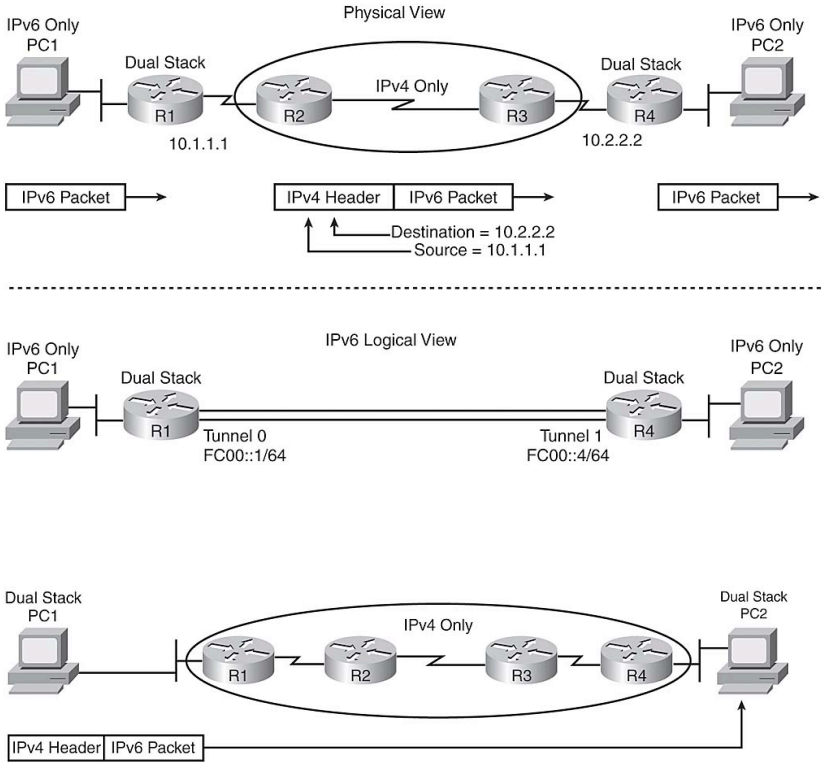
Configurado “por defecto” en algunos S.O. de escritorio.

Muchos usuarios pueden tener IPv6 sin saberlo.

Aproximadamente unas 10.000 Ips en el backbone de RedIRIS usan algún tipo de tunel.

Tipos de tunel.

- 6in4 (protocolo 41)
- TEREDO (NAT, UDP 3544)



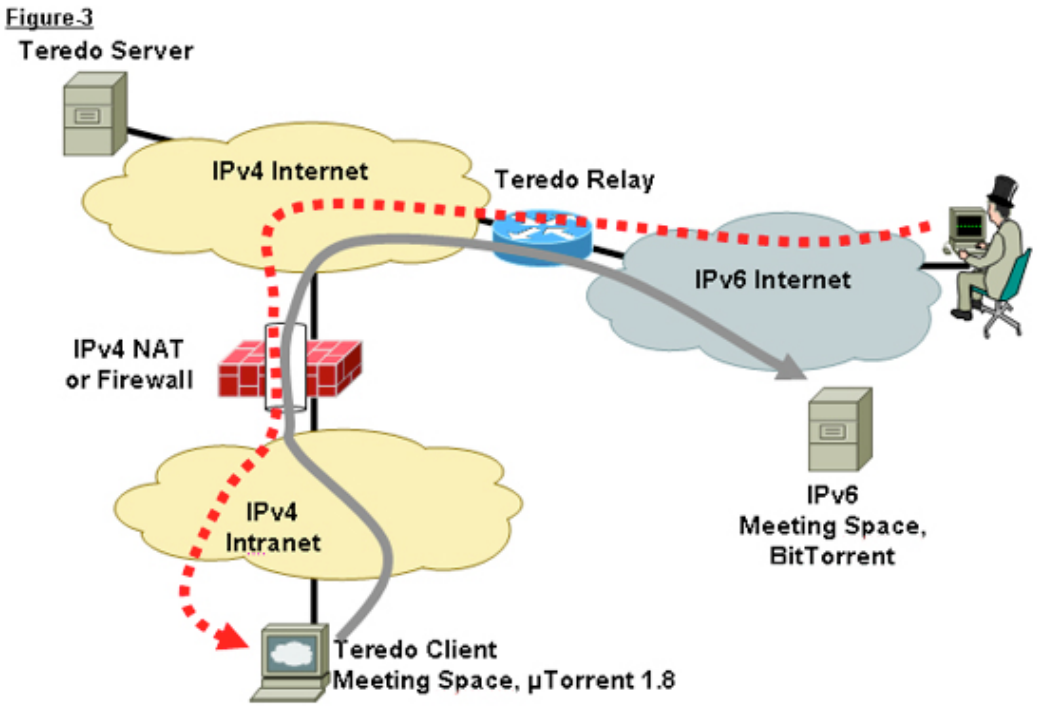
Problema: Tuneles IPv6

Los tuneles peden ser usados para acceder a equipos internos de la organización.

De no ser necesario es preciso bloquear el tráfico de tuneles IPv6

¿Cómo obtener direcciones IPv6 ?

- "ficheros de torrent"
- "blogs, comentarios de correos,etc



IPv6: Recomendaciones de seguridad

1. Comprobar que los dispositivos (Firewall, IDS, etc) soportan IPv6
2. Configurar políticas extrictas de registro (NetFlow) y filtros en las redes IPv6 desde el principio.
3. Monitorizar y bloquear tuneles si estos no son necesarios
4. Recordar que gran parte de los problemas no son debidos al nivel Red (TCP/IP) sino a vulnerabiliadas a nivel de aplicación y/o usuarios

IPv6 y los S.O.

La mayoría de los Sistemas Operativos soportan IPv6 desde hace tiempo:

- Linux RedHat, Ubuntu, debian, …..) , incluido en Kernel 1.X y 2.x
- Solaris
- Windows XP, Vista, 7

Incluso los exóticos (OpenVMS, AIX, ….)

Algunas características de IPTables no están soportadas.

Escaso soporte en aceleradores hardware a nivel de red.

IPv6 y el almacenamiento

IPv6 esta soportado en los proveedores de almacenamiento:

- NetAPP
- EMC
- HP

Protocolos de red:

- NetBios/SMB : problemas con algunos de los servicios
- NFS v4 : Sin soporte en NFS v3
- iSCSI : Iniciador 2.0

Puede ser necesario una actualización del S.O. para el soporte de IPv6.

Posibilidad de emplear direccionamiento "público" IPv6 para los dispositivos.

IPv6: Soporte hardware

Sistemas de gestión integrada

- KVM, apagados remotos de equipos. Soportados en aquellos basados en Linux.
- Ilom , (servidores SunOS), soportado

Arranque de equipos

- Aparte de la autoconfiguración vía Network Discovery Protocol
- PXE : sin estandarización sobre el uso de IPv6
- Bootp: Sin soporte IPv6
- tftp: Soporte IPv6 vía inetd
- dhcpd: Soporte IPv6

Herramientas de monotorización:

- Casi todas soportan IPv6
- ¿como se evalua si un equipo responde solamente en IPv4/IPv6 ?

IPv6: Soporte Hardware (II)

Sensores de control, domótica, alertas del SAID..

Servidores de impresión, impresoras en red.

Pantallas, proyectores de video, dispositivos de telefonía…

IPv6: Aplicaciones y desarrollos

¿Soportan las aplicaciones IPv6 ?

¿Incluidos los desarrollos propios ?

- A nivel de “sistemas” , alta de usuarios, direcciones, equipos…
- A nivel de gestión, registros de acceso en aplicación de nóminas, expedientes, etc

¡ MUCHAS GRACIAS! ☺