Grupo de Seguridad

Grupos de RedIRIS. Caceres

24 de Noviembre de 2014

seguridad@rediris.es

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMIA Y COMPETITIVIDAD
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
red.es
RedIRIS

- 16:00 Informe grupo de seguridad.
    - Actividades grupos IRIS-FORTI e IRIS-PAN
- Ataques de denegación de servicio
    - Filtros en enlaces a organizaciones
    - Autobloqueo de direcciones IP
    - Mitigación avanzada

16:25: Panel de discusión “Actuaciones con las Fuerzas de Seguridad del Estado”

- Pablo Alonso (UIT - Policia Nacional)
- Gustavo Rodriguez (US)
- Victoriano Giralt (UMA)

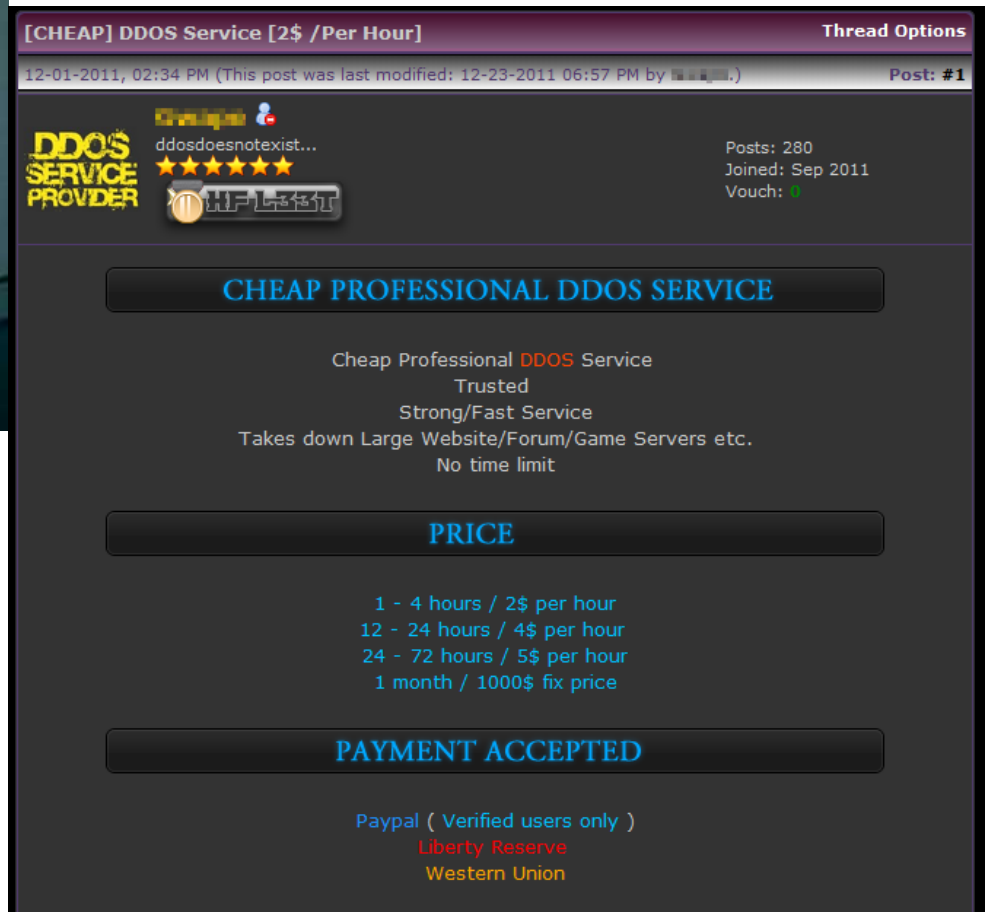
- 15:45: Estado del servicio IRIS-CERT

GRUPOS ESPECÍFICOS DE SEGURIDAD

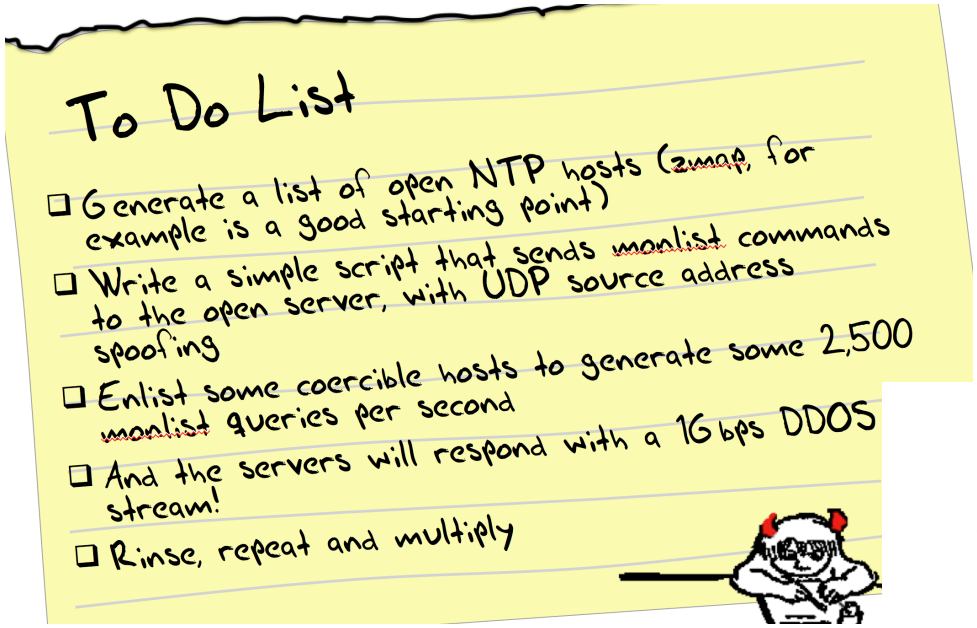
GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMIA Y COMPETITIVIDAD
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
red.es
RedIRIS

DENEGACIONES DE SERVICIO

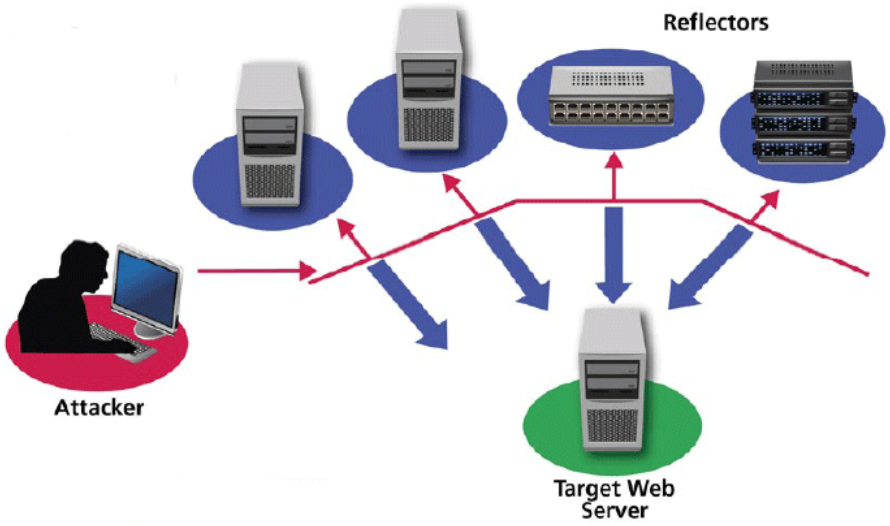
¿Hay ataques de denegación de servicio ?



¿qué se emplea ahora ? …

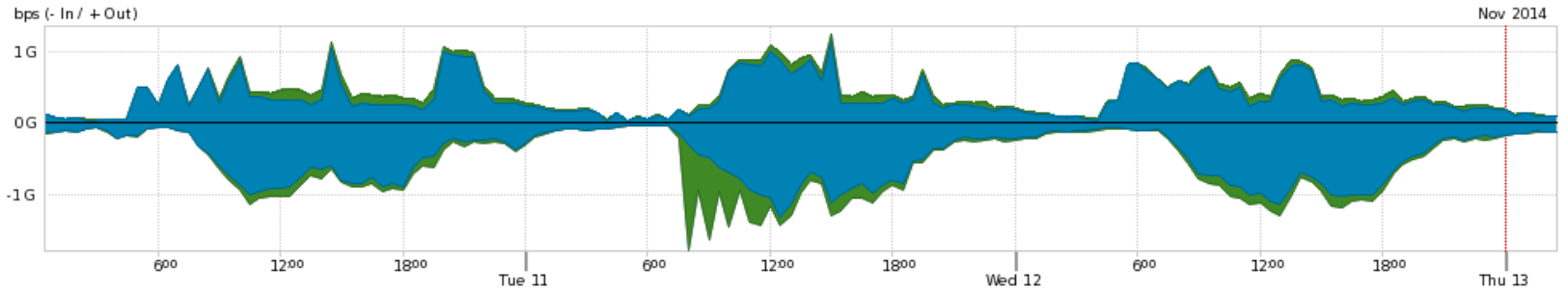


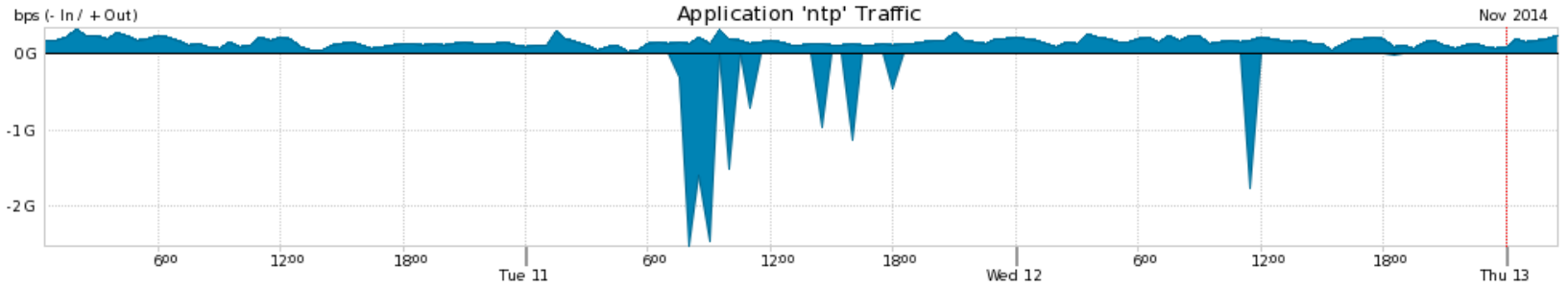
http://labs.apnic.net/blabs/?p=464



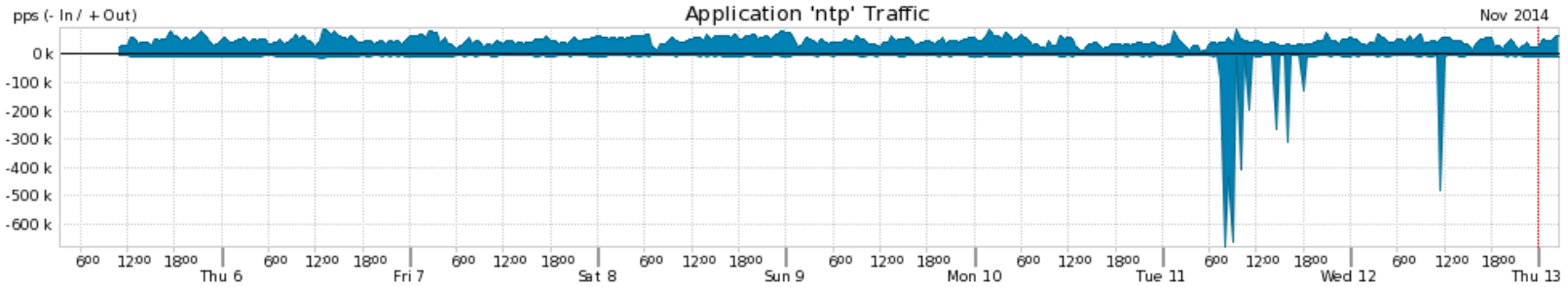
http://blog.elhacker.net/2014/06/udp-flood-inundacion-reflection-attack-ataque.html

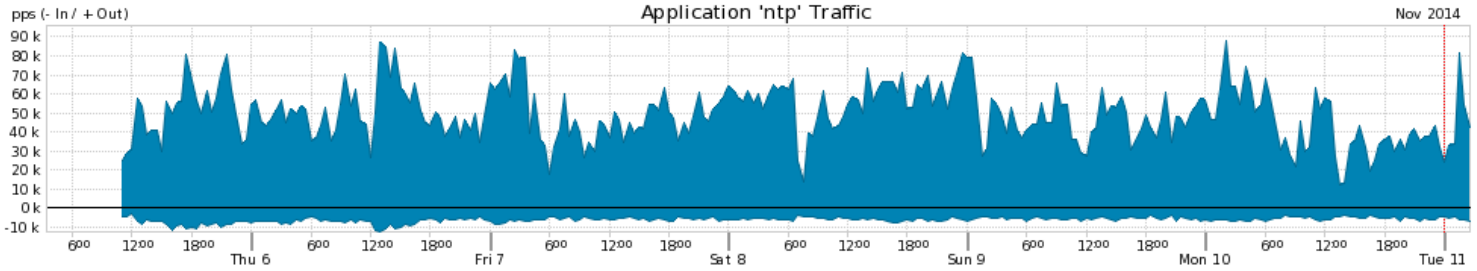
Ataques NTP Nov 2014





Ataques NTP Nov 2014 (II)





GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMIA Y COMPETITIVIDAD
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
red.es
RedIRIS

SERVICIOS DE MITIGACION EN EL TRONCAL.

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMIA Y COMPETITIVIDAD
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
red.es
RedIRIS

Protección ante un un DDOS en organizaciones ..

- Siguiendo la guía CCN-STIC 820: Protección contra DDOS:
  - Estar preparados.
    - ¿Qué servicios hay que proteger ?
    - ¿Cual es su impacto ?
    - ¿Que hay que hacer para prevenirlo ?
  - Conocer tu tráfico (análisis y monitorización)
  - Conocer a tu ISP (que te podrá ayudar)

- Filltros no permanentes
- Auto eliminacion de direcciones IP
- Diferenciación avanzada de trafico

Definiciones

ejemplo: activos – usuario

activo	editar	current	target
ACTIVOS			
[essential] Activos esenciales			
[B] Capa de negocio			
[IS] Servicios internos			
[E] Equipamiento		on	
[SW] Aplicaciones			
[HW] Equipos		on	
[PC] Puestos de trabajo	editar		
[SRV] Servidor	editar	on	
[COM] Comunicaciones			
[AUX] Elementos auxiliares			
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			

1 2 3 4 5

Análisis de Riesgos

Filtros temporales

- Ante amenazas temporales y puntuales de tráfico.
- Solamente para tráfico muy caracterizado.
  - Permitir tráfico a AA.BB.CC.DD / 80
  - Permitir trafico a XX.XX.XX.XX / puertos AA/ BB
  - Denegar el resto
  - Valido para trafico de servidores
- Una vez acabada la amenaza se eliminan los filtros.

Filtros temporales I.

1. Solicitar a seguridad@rediris.es documento informativo.

2. Rellenar el documento indicando los puertos a filtrar

Filtros temporales II

1. Configuración en el enlace de acceso al centro de los filtros unos días antes del problema.
2. Monitorización en el periodo del ataque del enlace.

Filtros temporales III

1. Eliminación de los filtros una vez acabado el periodo de ataque.
2. Conservación de los filtros (fuera del router) como previsión ante otros ataques.
3. Base para otros servicios de mitigación

Estado del servicio

- Probado en diversas situaciones a lo largo de 1994.
  - Filtros realizados para 2 instituciones, aplicados 4 veces (3:1)
- Efectivo contra DDOS contra servidores empleando reflexión de trafico
- No efectivo contra DDOS imprevistos.
- No valido contra DDOS no volumétricos o empleando puertos de servicio validos.

SELF IP blocking

Autobloqueo de direcciones IP de la organización en el bloqueo

Solicitud por parte del PER

- Rango IP
- Router BGP de organización.

SELF IP blocking

Autobloqueo de direcciones IP de la organización en el bloqueo

Establecimiento sesión BGP

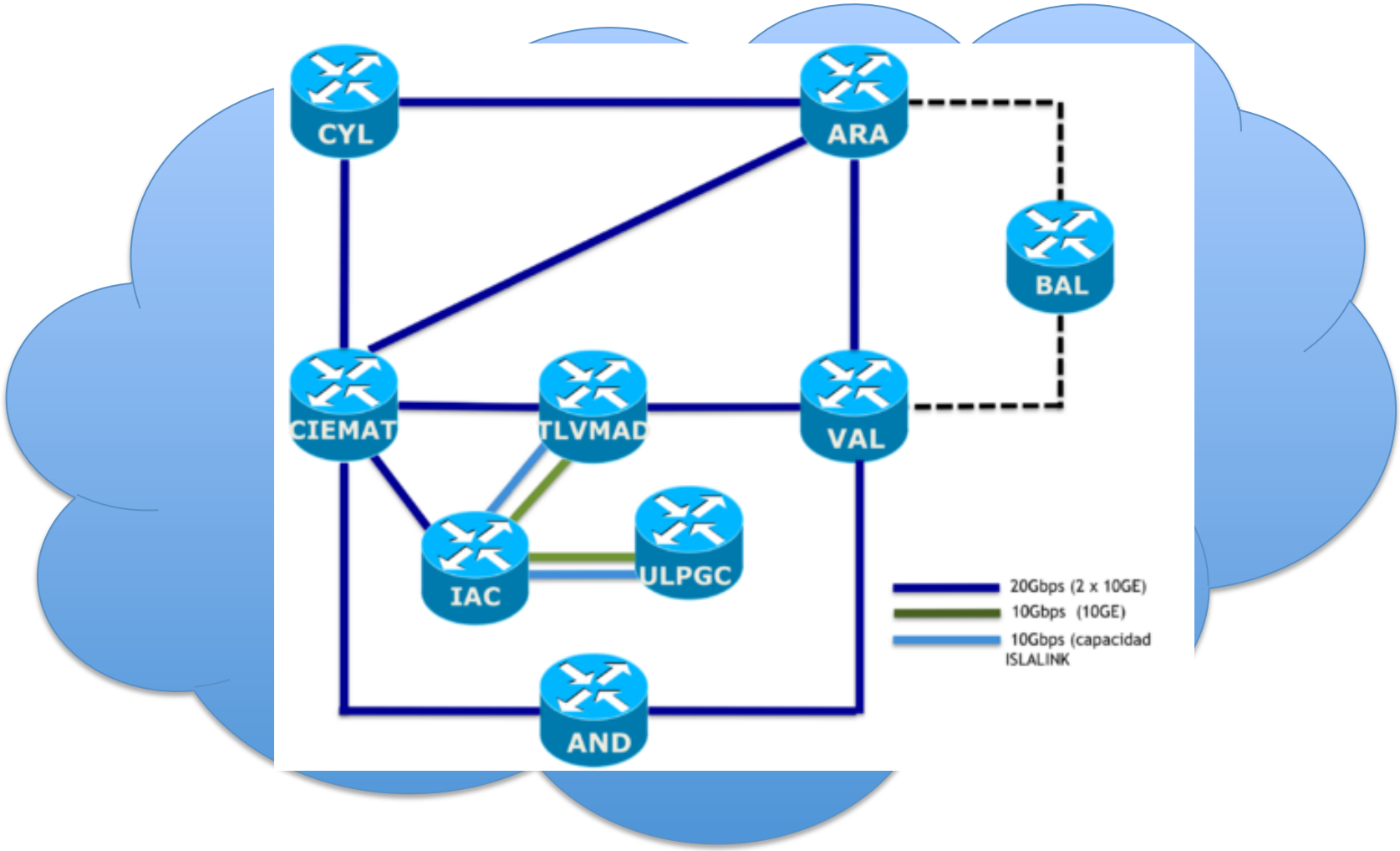
- Solamente /32
- Limitado a rangos de la organización
- Limitado a blackhole

SELF IP blocking

Autobloqueo de direcciones IP de la organización en el bloqueo

Ante un problema la institución realiza el anuncio de la dirección IP.

Red Troncal de RedIRIS

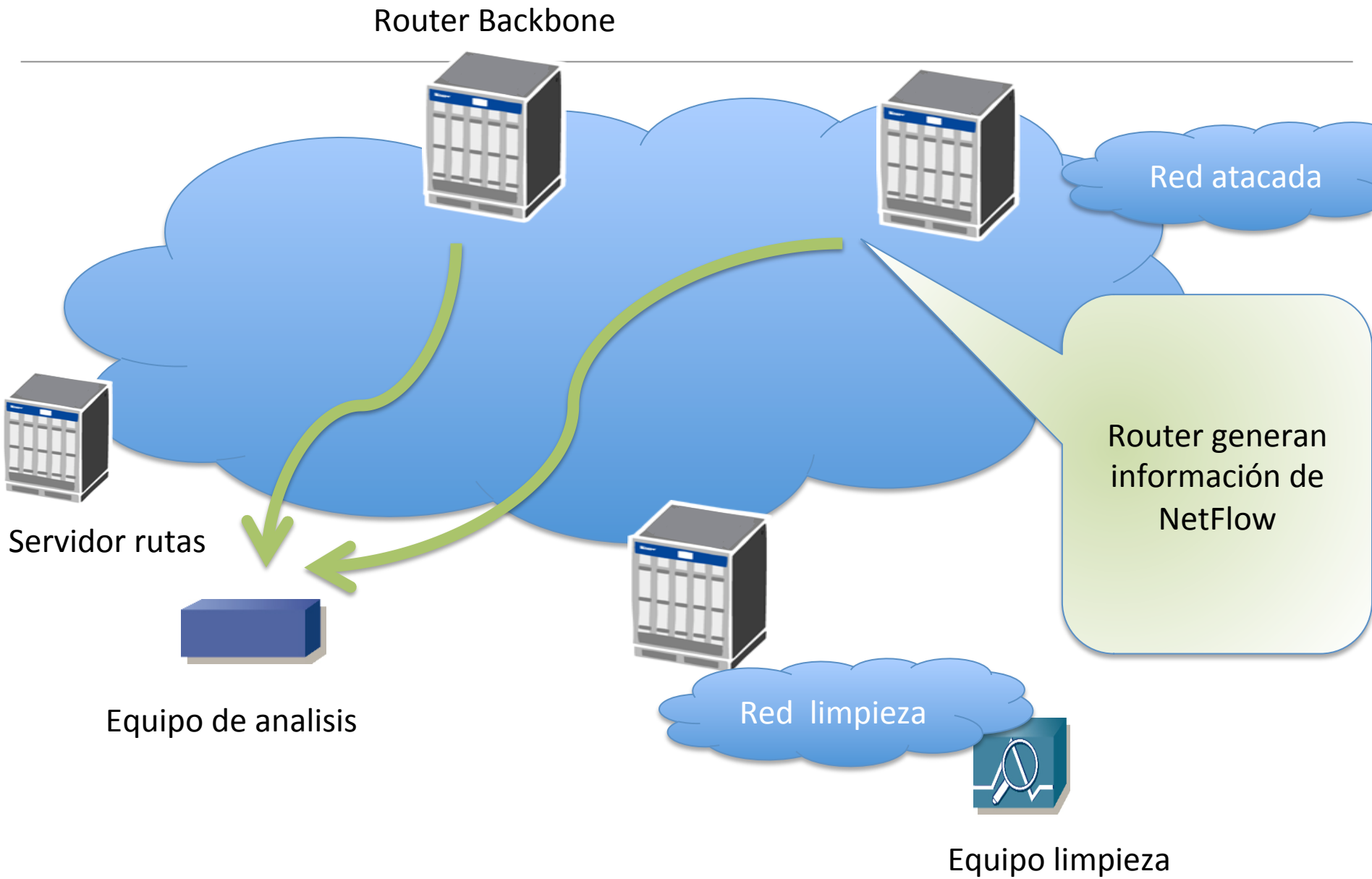


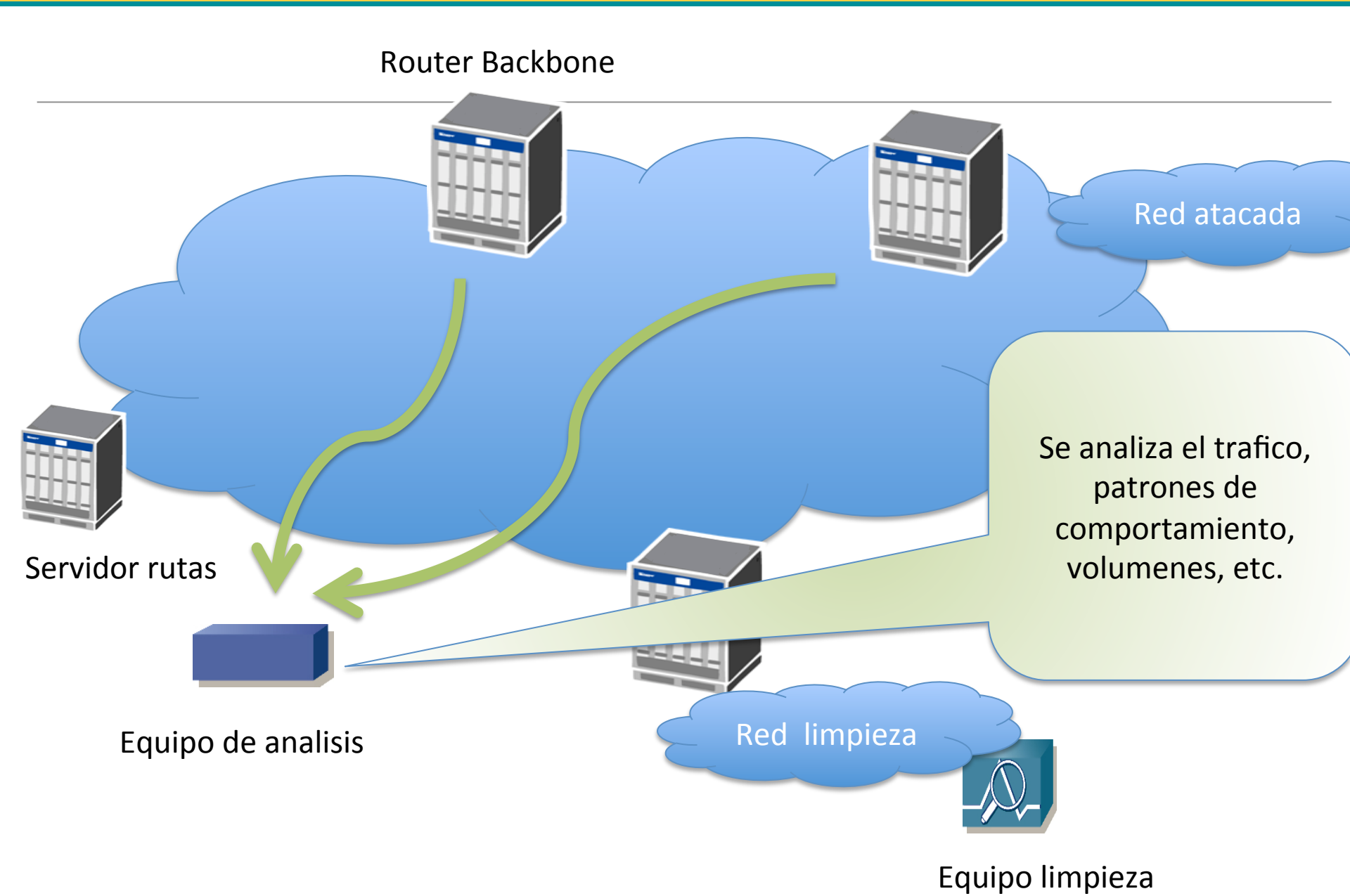
Self IP blocking.

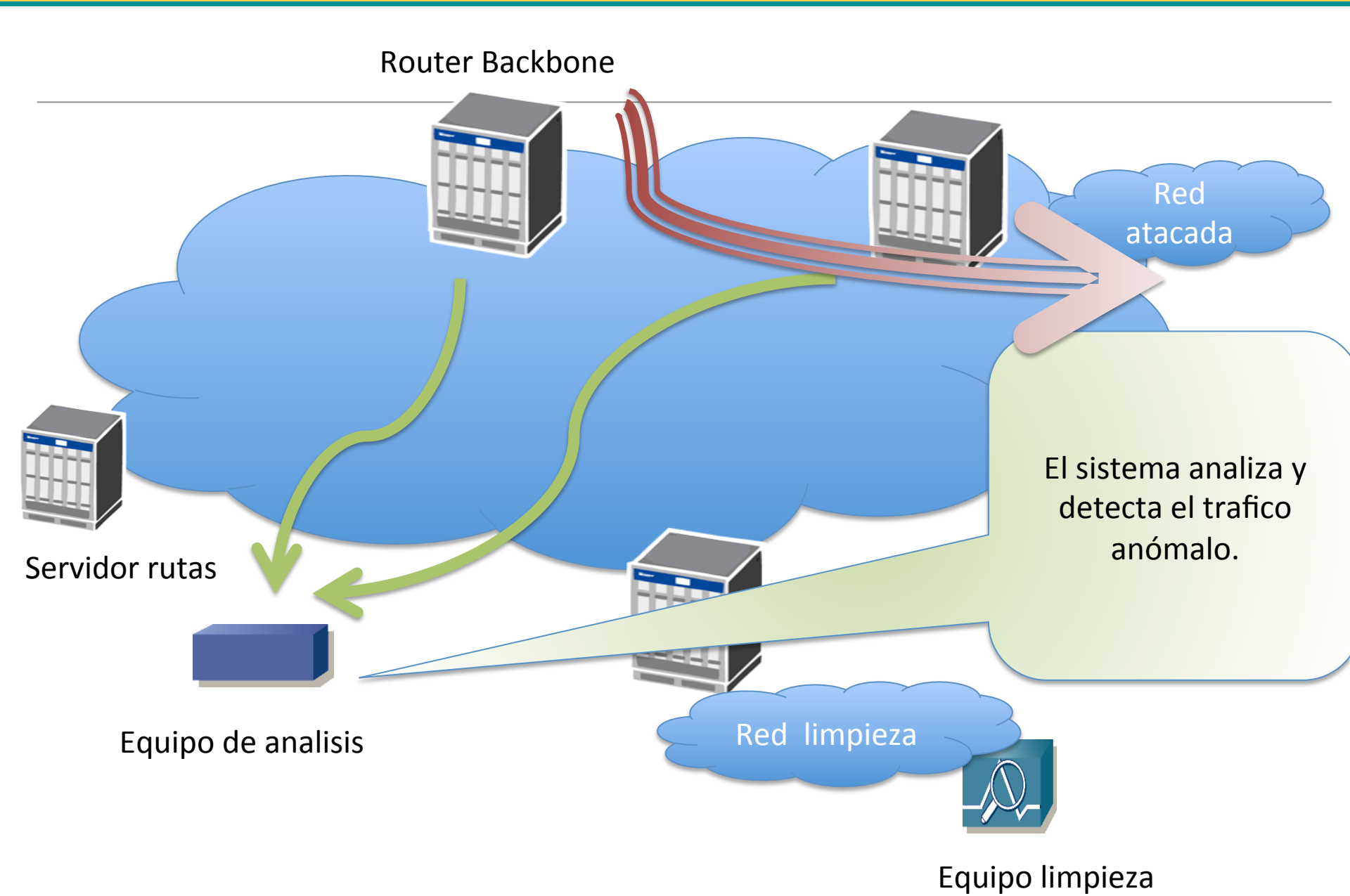
- Por dificultades técnicas el piloto del servicio todavía no esta disponible.
  - Pruebas previstas en diciembre
  - Solicitudes a partir de Febrero

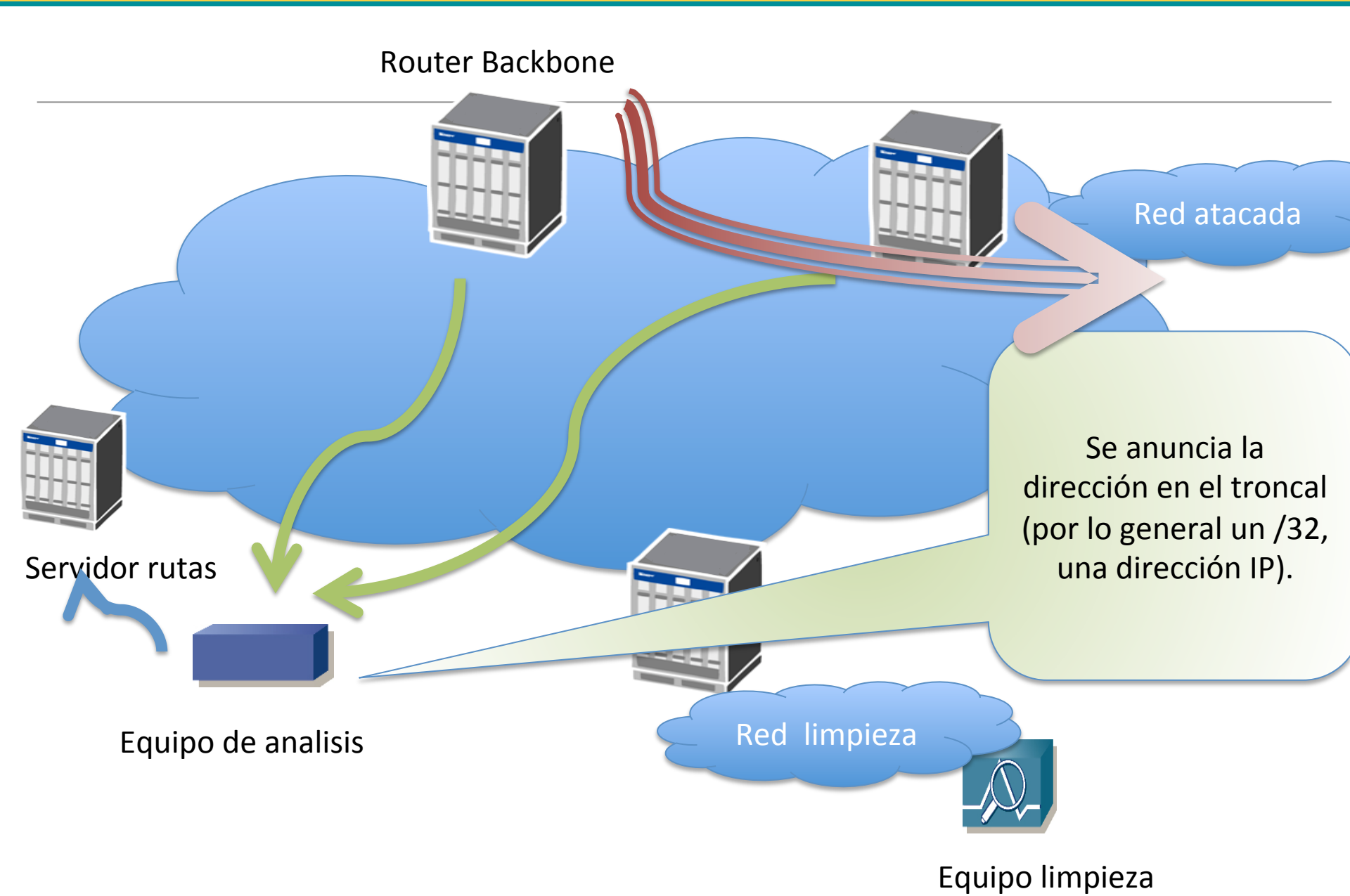
- ¿quién podrá solicitarlo ?

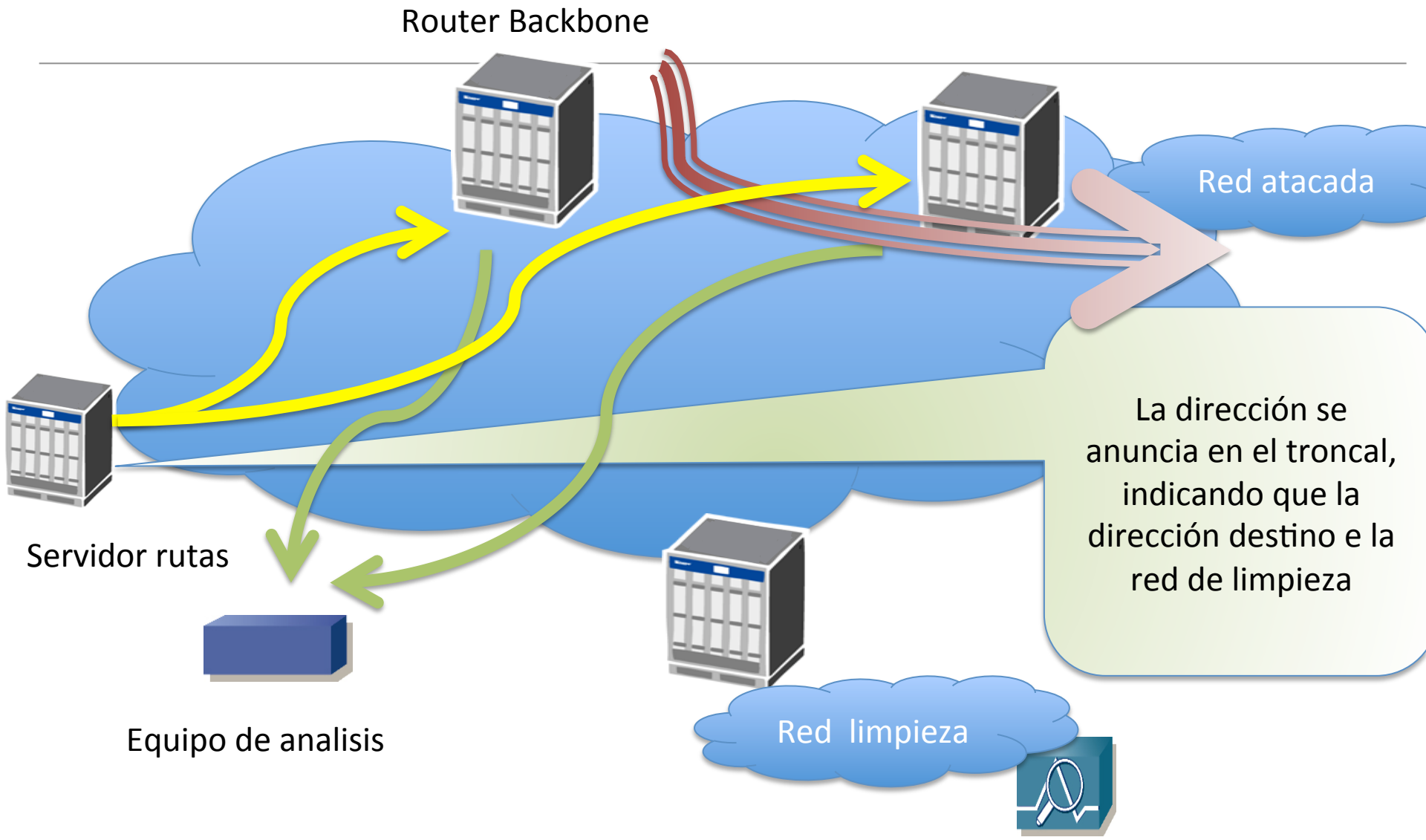
  Cualquier institución conectada a RedIRIS

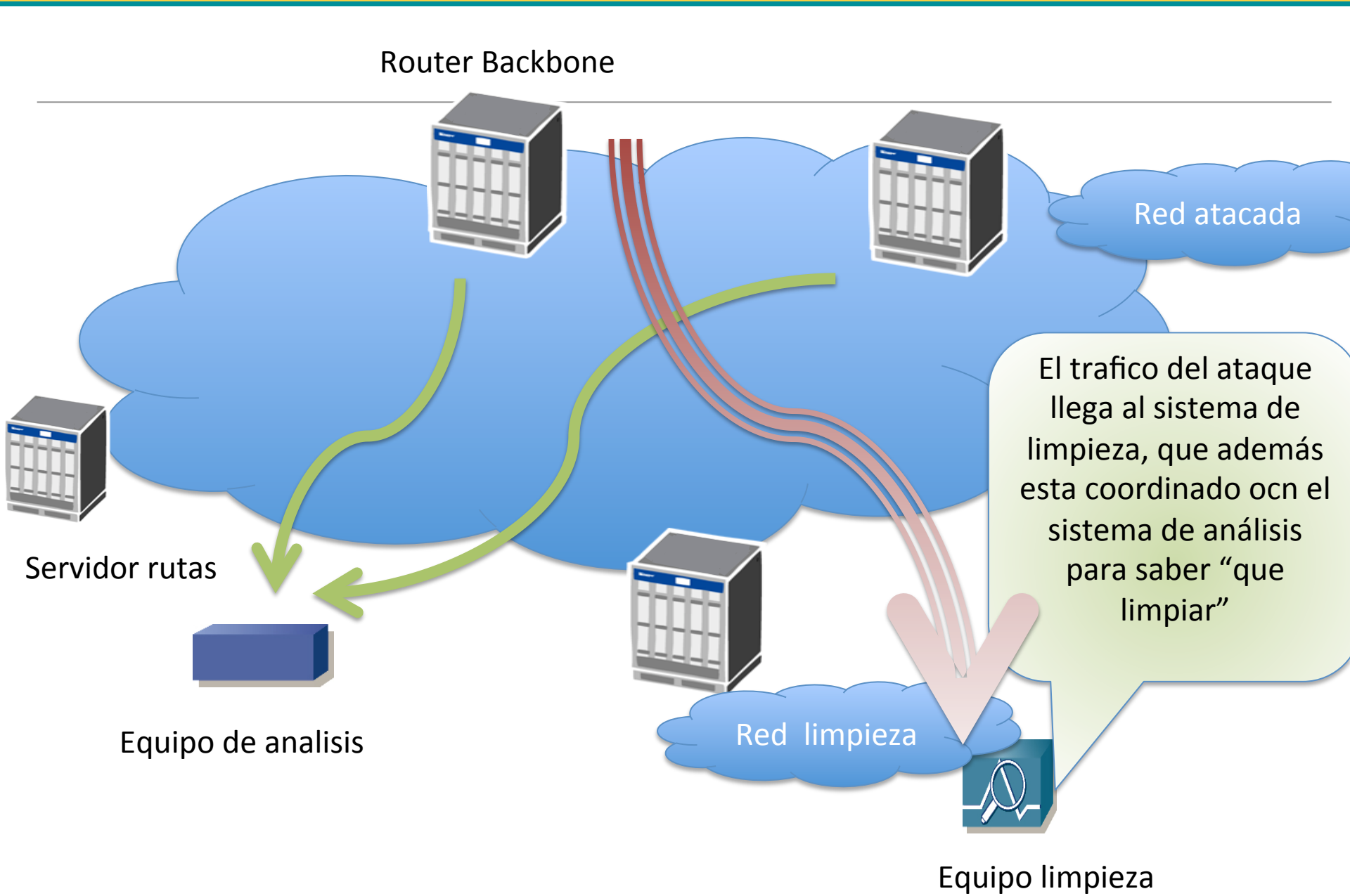

Router Backbone
Red atacada
Router generan información de NetFlow
Servidor rutas
Equipo de analisis
Red limpieza
Equipo limpieza


Router Backbone
Red atacada
Servidor rutas
Se analiza el trafico, patrones de comportamiento, volumenes, etc.
Equipo de analisis
Red limpieza
Equipo limpieza

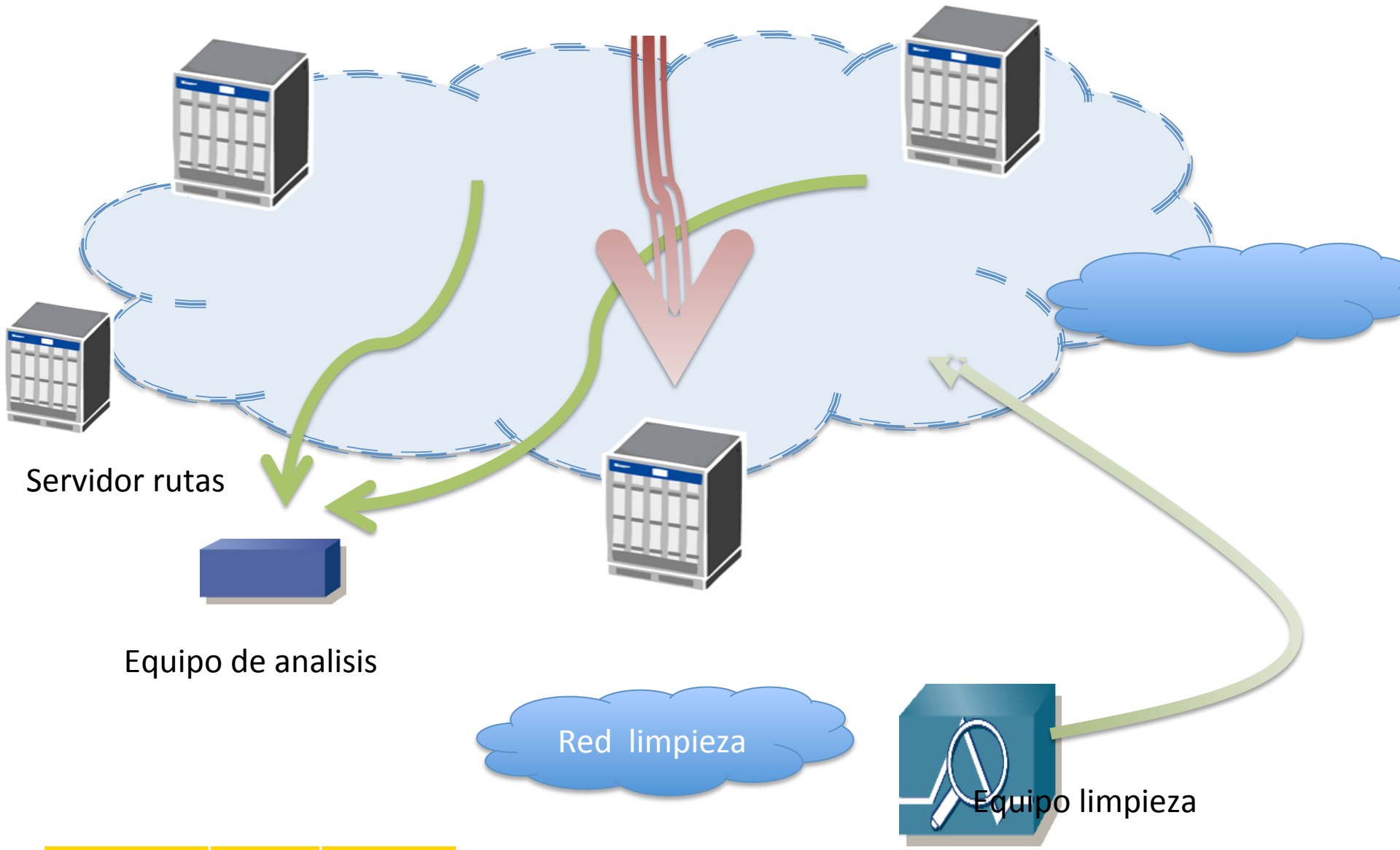

Router Backbone
Red atacada
El sistema analiza y detecta el trafico anómalo.
Servidor rutas
Equipo de analisis
Red limpieza
Equipo limpieza

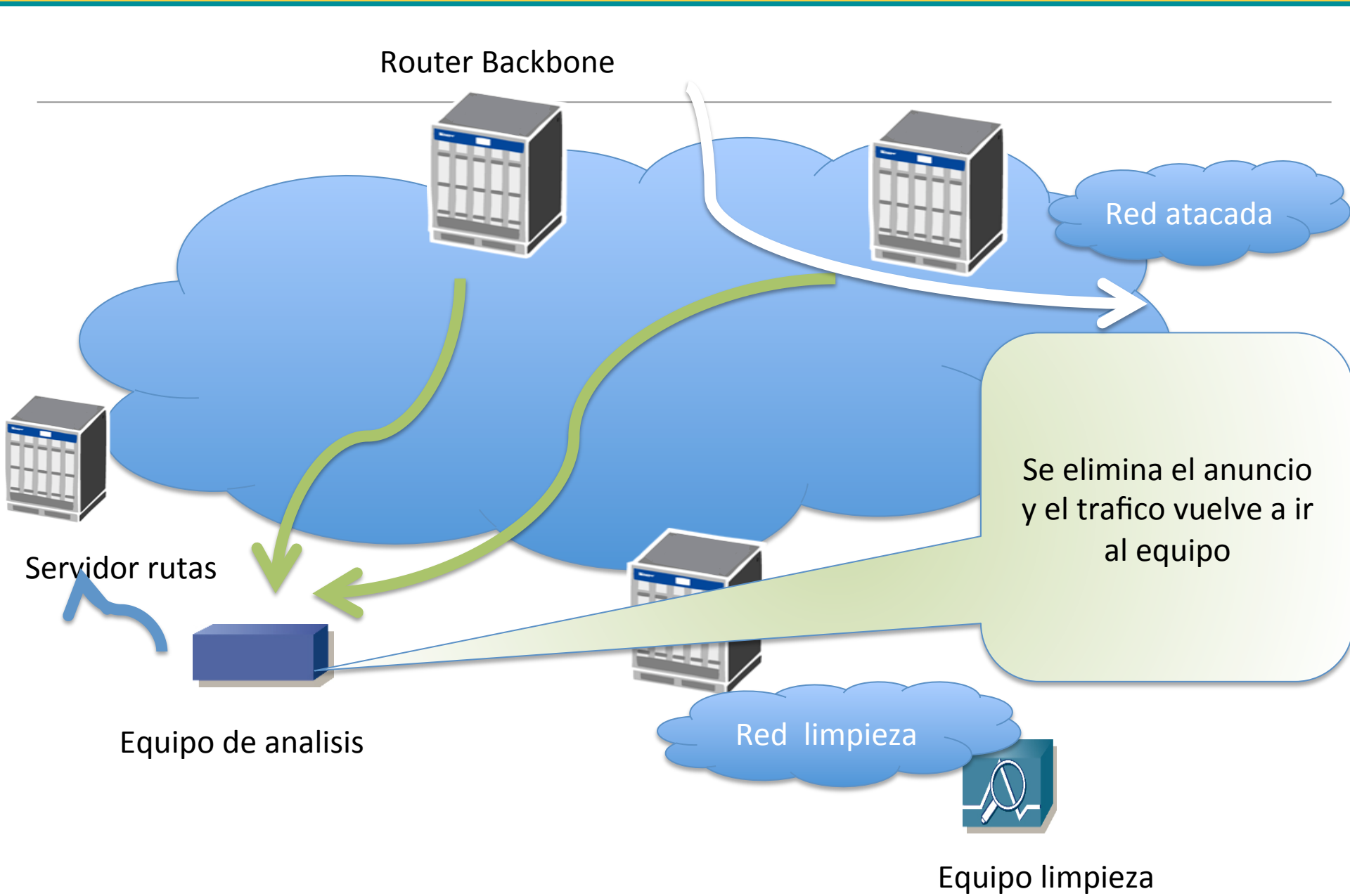

Router Backbone
Red atacada
Se anuncia la dirección en el troncal (por lo general un /32, una dirección IP).
Servidor rutas
Equipo de analisis
Red limpieza
Equipo limpieza


Router Backbone
Red atacada
La dirección se anuncia en el troncal, indicando que la dirección destino e la red de limpieza
Servidor rutas
Equipo de analisis
Red limpieza
Equipo limpieza


Router Backbone
Red atacada
El trafico del ataque llega al sistema de limpieza, que además esta coordinado ocn el sistema de análisis para saber “que limpiar”
Servidor rutas
Equipo de analisis
Red limpieza
Equipo limpieza

Router Backbone




Router Backbone
Red atacada
Se elimina el anuncio y el trafico vuelve a ir al equipo
Servidor rutas
Equipo de analisis
Red limpieza
Equipo limpieza

PANEL DE DISCUSION

- ¿qué obligaciones tiene una organización afiliada con las FSE ?
- ¿Qué tipo de peticiones y requerimientos se reciben ?
- ¿Cómo actuar cuando se detecta una actividad ilicita en las organizaciones ?
- ¿cuáles son los miedos ante las amenazas ?

Panel.

Pablo Alonso , Policía Nacional

Victoriano Giralt, Universidad de Málaga

Gustavo Rodriguez , Universidad de Sevilla

SERVICIO IRIS-CERT

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMIA Y COMPETITIVIDAD
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
red.es
Red IRIS

¿qué ha sido IRIS-CERT?

- IRIS-CERT se ha usado tradicionalmente para referir múltiples funciones/servicios/personas.
  - Ha existido ambigüedad y múltiples usos.
- ¿a que nos referimos con IRIS-CERT?
  - IRIS-CERT@listserv.rediris.es : Lista de coordinación sobre temas de seguridad de la comunidad RedIRIS.
  - IRIS-CERT, http://www.rediris.es/cert , Equipo de Respuesta a incidentes de Seguridad de RedIRIS , ámbito.
  - IRIS-CERT, http://www.rediris.es/cert/ih , Servicio de atención de incidentes de seguridad a las instituciones afiliadas a RedIRIS

Servicio de atención de seguridad a las instituciones afiliadas.

- En 2013, la dirección de Red.es decide que el servicio de atención de incidentes de la comunidad de RedIRIS debe ser gestionado por INTECO (ahora INCIBE).
- Desde 2014, el servicio de atención a incidentes de las instituciones afiliadas a RedIRIS (nivel 1 y nivel 2) ha sido operado por técnicos de INTECO (desde la herramienta de RedIRIS).
- La dirección del servicio de atención a incidentes de seguridad de las instituciones reside en RedIRIS, quién asegurará:
  - Que el servicio se presta en las condiciones que estipula RedIRIS.
  - Que el servicio mantiene la calidad con la que se venía prestando, asegurando el cumplimiento de la Norma vigente para la prestación del servicio.

En 2015…

- INCIBE (INTECO) ha decidido migrar a su plataforma de gestión de incidentes, que hasta ahora se realizaba desde la plataforma de RedIRIS:
  - El servicio de atención a incidentes de seguridad a las instituciones afiliadas es un servicio de RedIRIS a su comunidad.
  - El servicio de atención a incidentes de seguridad a las instituciones afiliadas seguirá operado por INCIBE.
  - El servicio cambiará la dirección cert@rediris.es a iris@cert.inteco.es / iris@cert.incibe.es una vez se migre la plataforma.
- Los cambios relativos al servicio de atención a incidentes de las instituciones serán notificados por la lista IRIS-CERT.

Lista de Seguridad

- IRIS-CERT se mantiene como lista de coordinación para temas de seguridad, solamente de la comunidad.
  - Aspectos específicos para no saturar tecniris@
  - Anuncios e información del equipo de respuesta de RedIRIS

El equipo de seguridad

- RedIRIS sigue manteniendo los servicios de seguridad a las instituciones afiliadas:
  - Gestión de incidentes de seguridad a las instituciones (IRIS-CERT).
    - Gestión estratégica depende de RedIRIS.
    - Operación realizada por Incibe.
- RedIRIS gestiona la seguridad que afecte a la infraestructura de RedIRIS.
- Cambio de nombre en 2015 para evitar ambigüedades con el servicio de atención de incidentes
  - Seguridad en el equipamiento de RedIRIS
    - Servidores
    - Infraestructura de comunicaciones.
  - Desarrollo de nuevos servicios de seguridad a las instituciones afiliadas
  - Evaluación de los servicios de seguridad prestados por otras partes a RedIRIS

Nuevo equipo de seguiridad

¡Muchas gracias!

Más de 25 años al servicio de la investigación