

Grupo de Seguridad

Grupos de RedIRIS. Cáceres

24 de Noviembre de 2014

seguridad@rediris.es

-
- 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

DENEGACIONES DE SERVICIO

¿Hay ataques de denegación de servicio ?



[CHEAP] DDOS Service [2\$ /Per Hour] Thread Options

12-01-2011, 02:34 PM (This post was last modified: 12-23-2011 06:57 PM by [user].) Post: #1

DDOS SERVICE PROVIDER ddosdoesnotexist... ★★★★★ WFL

Posts: 280
Joined: Sep 2011
Vouch: [green icon]

CHEAP PROFESSIONAL DDOS SERVICE

Cheap Professional **DDOS** Service
Trusted
Strong/Fast Service
Takes down Large Website/Forum/Game Servers etc.
No time limit

PRICE

1 - 4 hours / 2\$ per hour
12 - 24 hours / 4\$ per hour
24 - 72 hours / 5\$ per hour
1 month / 1000\$ fix price

PAYMENT ACCEPTED

Paypal (Verified users only)
Liberty Reserve
Western Union

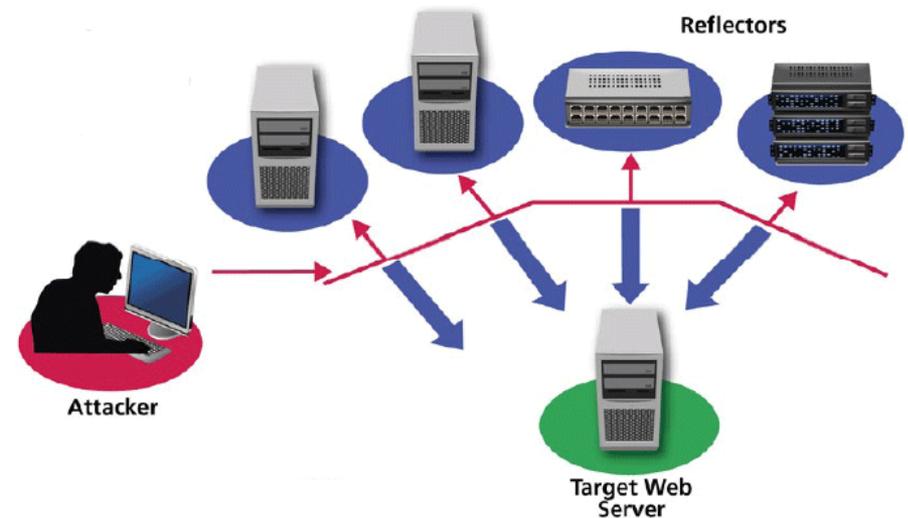
¿qué se emplea ahora ? ...

To Do List

- ❑ Generate a list of open NTP hosts (zmap, for example is a good starting point)
- ❑ Write a simple script that sends manlist commands to the open server, with UDP source address spoofing
- ❑ Enlist some coercible hosts to generate some 2,500 manlist queries per second
- ❑ And the servers will respond with a 1Gbps DDOS stream!
- ❑ Rinse, repeat and multiply

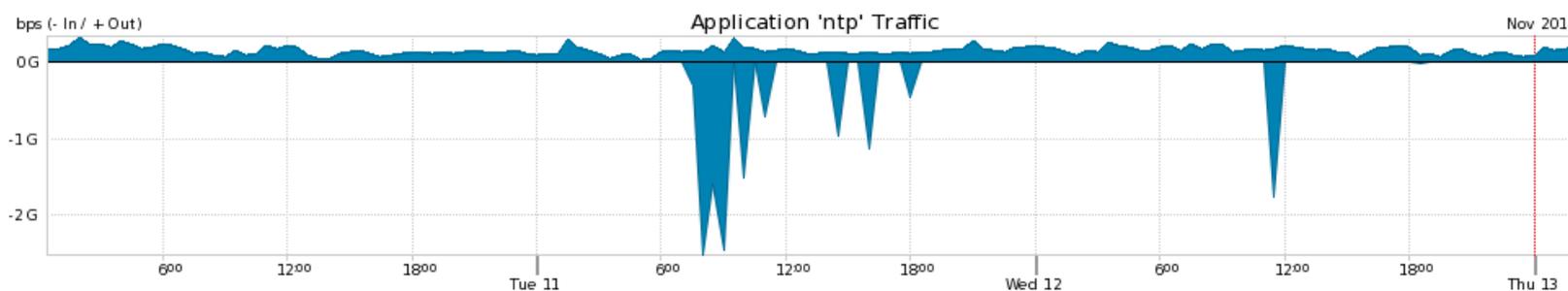
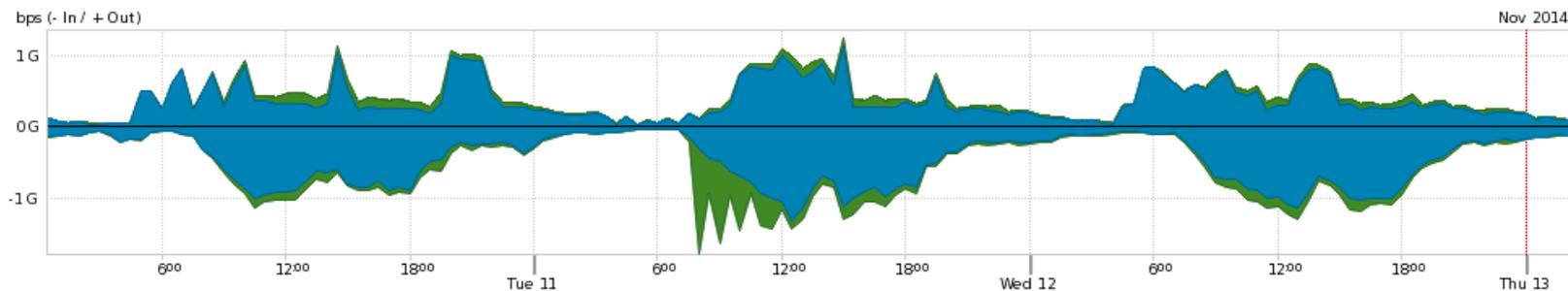


<http://labs.apnic.net/blabs/?p=464>

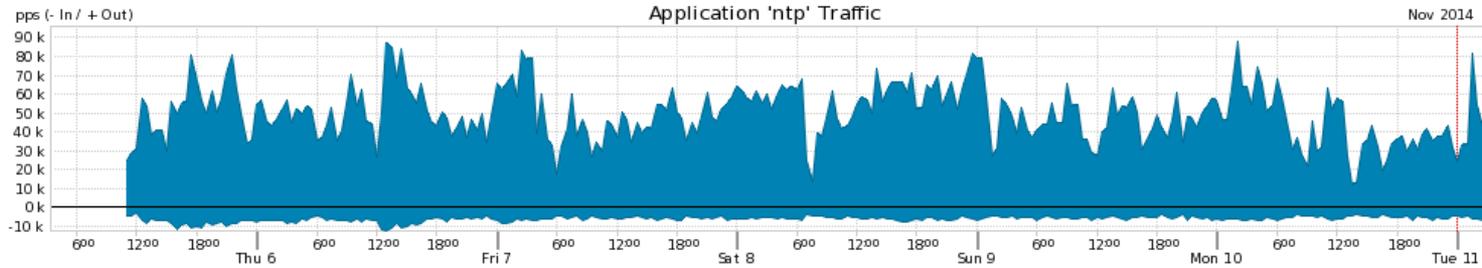
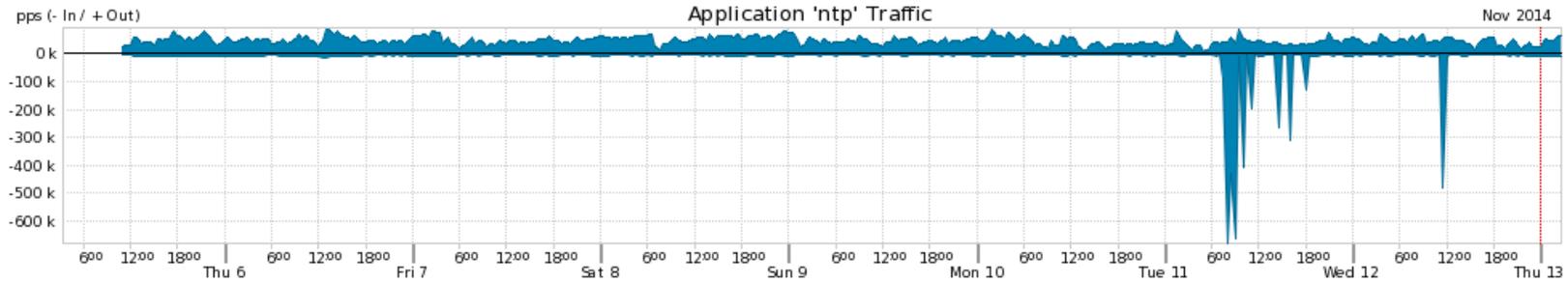


<http://blog.elhacker.net/2014/06/udp-flood-inundacion-reflection-attack-ataque.html>

Ataques NTP Nov 2014



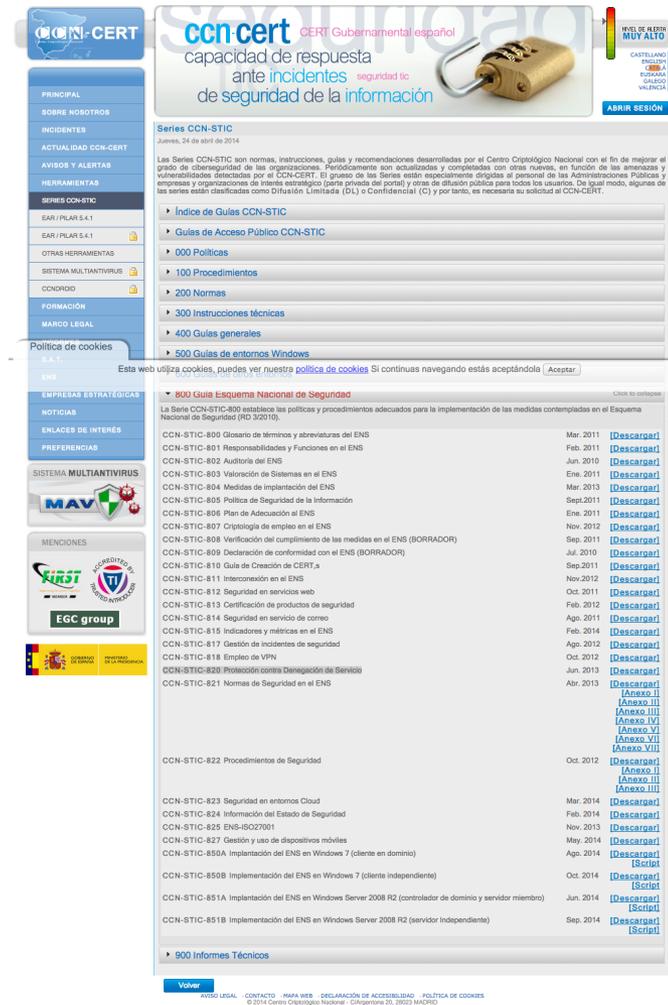
Ataques NTP Nov 2014 (II)



SERVICIOS DE MITIGACION EN EL TRONCAL.

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)



CCN-CERT CERT Gubernamental español
capacidad de respuesta ante incidentes seguridad ic de seguridad de la información

SERIES CCN-STIC
Jueves, 24 de abril de 2014

Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT. El grupo de las Series están especialmente dirigidas al personal de las Administraciones Públicas y empresas y organizaciones de Internet estratégico (para privada del portal) y otras de difusión pública para todos los usuarios. De igual modo, algunas de las series están clasificadas como Difusión Limitada (DL) o Confidencial (C) y por tanto, es necesaria su solicitud al CCN-CERT.

- ▶ Índice de Guías CCN-STIC
- ▶ Guías de Acceso Público CCN-STIC
- ▶ 000 Políticas
- ▶ 100 Procedimientos
- ▶ 200 Normas
- ▶ 300 Instrucciones técnicas
- ▶ 400 Guías generales
- ▶ 500 Guías de entornos Windows

Esta web utiliza cookies, puedes ver nuestra [política de cookies](#) Si continuas navegando estás aceptándola

800 Guía Esquema Nacional de Seguridad

La Serie CCN-STIC-800 establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el Esquema Nacional de Seguridad (RD 3/2010).

CCN-STIC	Descripción	Fecha	Acción
CCN-STIC-800	Glosario de términos y abreviaturas del ENS	Mar. 2011	[Descargar]
CCN-STIC-801	Responsabilidades y Funciones en el ENS	Feb. 2011	[Descargar]
CCN-STIC-802	Auditoría del ENS	Jun. 2010	[Descargar]
CCN-STIC-803	Validación de Sistemas en el ENS	Ene. 2011	[Descargar]
CCN-STIC-804	Medidas de implantación del ENS	Mar. 2013	[Descargar]
CCN-STIC-805	Política de Seguridad de la Información	Sept. 2011	[Descargar]
CCN-STIC-806	Plan de Adecuación al ENS	Ene. 2011	[Descargar]
CCN-STIC-807	Criptología de empleo en el ENS	Nov. 2012	[Descargar]
CCN-STIC-808	Verificación del cumplimiento de las medidas en el ENS (BORRADOR)	Sept. 2011	[Descargar]
CCN-STIC-809	Declaración de conformidad con el ENS (BORRADOR)	Jul. 2010	[Descargar]
CCN-STIC-810	Guía de Creación de CERT.s	Sept. 2011	[Descargar]
CCN-STIC-811	Interconexión en el ENS	Nov. 2012	[Descargar]
CCN-STIC-812	Seguridad en servicios web	Oct. 2011	[Descargar]
CCN-STIC-813	Certificación de productos de seguridad	Feb. 2012	[Descargar]
CCN-STIC-814	Seguridad en servicio de correo	Ago. 2011	[Descargar]
CCN-STIC-815	Indicadores y métricas en el ENS	Feb. 2014	[Descargar]
CCN-STIC-817	Gestión de incidentes de seguridad	Ago. 2012	[Descargar]
CCN-STIC-818	Empiezo de VPN	Oct. 2012	[Descargar]
CCN-STIC-820	Protección contra Denegación de Servicios	Jun. 2013	[Descargar]
CCN-STIC-821	Normas de Seguridad en el ENS	Abr. 2013	[Descargar] [Anexo I] [Anexo II] [Anexo III] [Anexo IV] [Anexo V] [Anexo VI] [Anexo VII]
CCN-STIC-822	Procedimientos de Seguridad	Oct. 2012	[Descargar] [Anexo I] [Anexo II] [Anexo III]
CCN-STIC-823	Seguridad en entornos Cloud	Mar. 2014	[Descargar]
CCN-STIC-824	Información del Estado de Seguridad	Feb. 2014	[Descargar]
CCN-STIC-825	ENS-ISO27001	Nov. 2013	[Descargar]
CCN-STIC-827	Gestión y uso de dispositivos móviles	May. 2014	[Descargar]
CCN-STIC-850A	Implantación del ENS en Windows 7 (cliente en dominio)	Ago. 2014	[Descargar] [Script]
CCN-STIC-850B	Implantación del ENS en Windows 7 (cliente independiente)	Oct. 2014	[Descargar] [Script]
CCN-STIC-851A	Implantación del ENS en Windows Server 2008 R2 (controlador de dominio y servidor miembro)	Jun. 2014	[Descargar] [Script]
CCN-STIC-851B	Implantación del ENS en Windows Server 2008 R2 (servidor independiente)	Sept. 2014	[Descargar] [Script]

▶ 900 Informes Técnicos

[Volver](#)

[AVISO LEGAL](#) [CONTACTO](#) [MAPA WEB](#) [DECLARACIÓN DE ACCESIBILIDAD](#) [POLÍTICA DE COOKIES](#)
© 2014 Centro Criptológico Nacional - C/Argentea 20, 28023 MADRID

-
- Filtros 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		in	
▶ [PC] Puestos de trabajo	editar		
▶ [SRV] Servidor	editar	on	
▶ [COM] Comunicaciones			
▶ [AUX] Elementos auxiliares			
▶ [SS] Servicios subcontratados			
▶ [I] Instalaciones			
▶ [P] Personal			

1 3 2 4 5

- 1 +

😊 ? ☹️

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 tráfico 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 tráfico
- 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



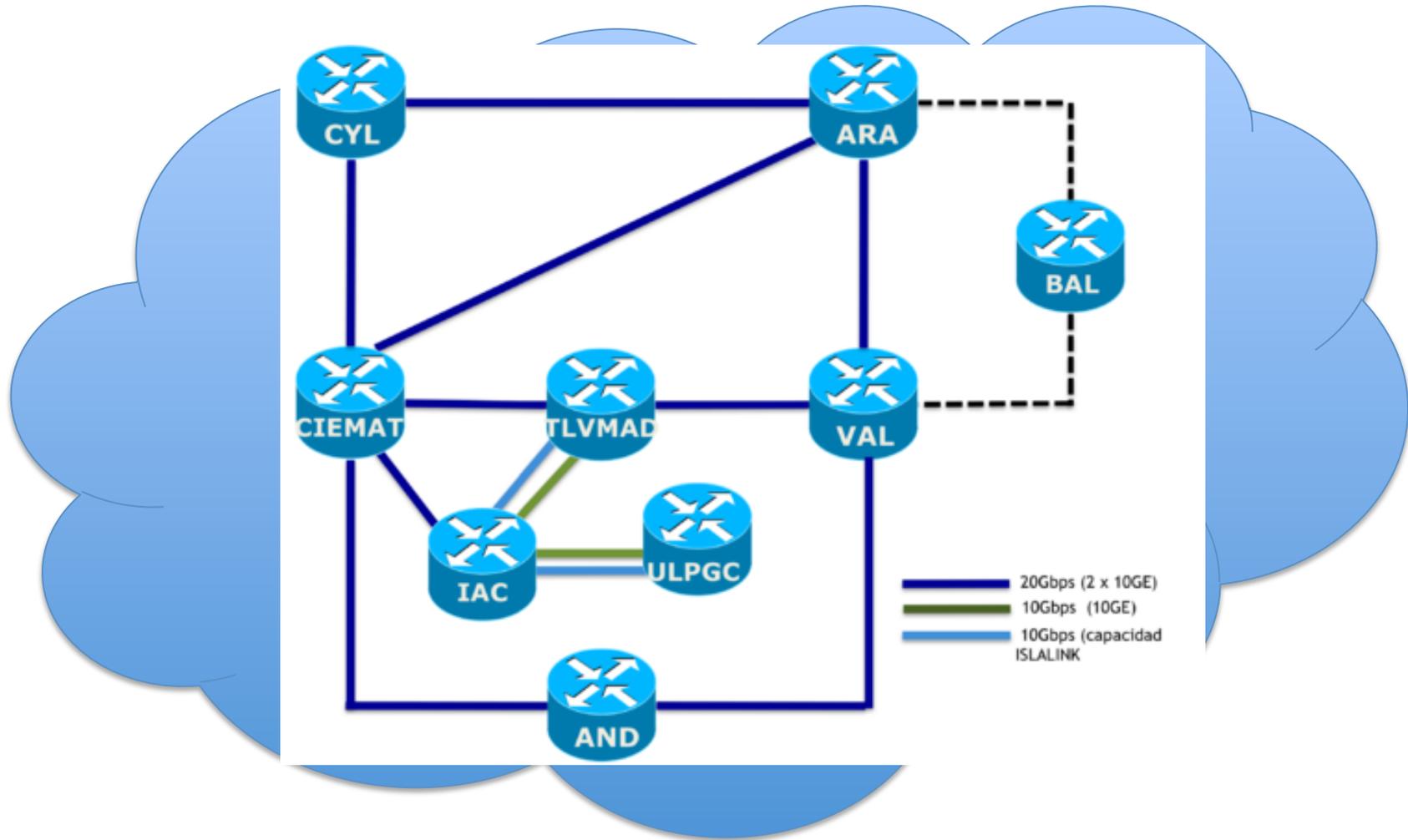
SELF IP blocking

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

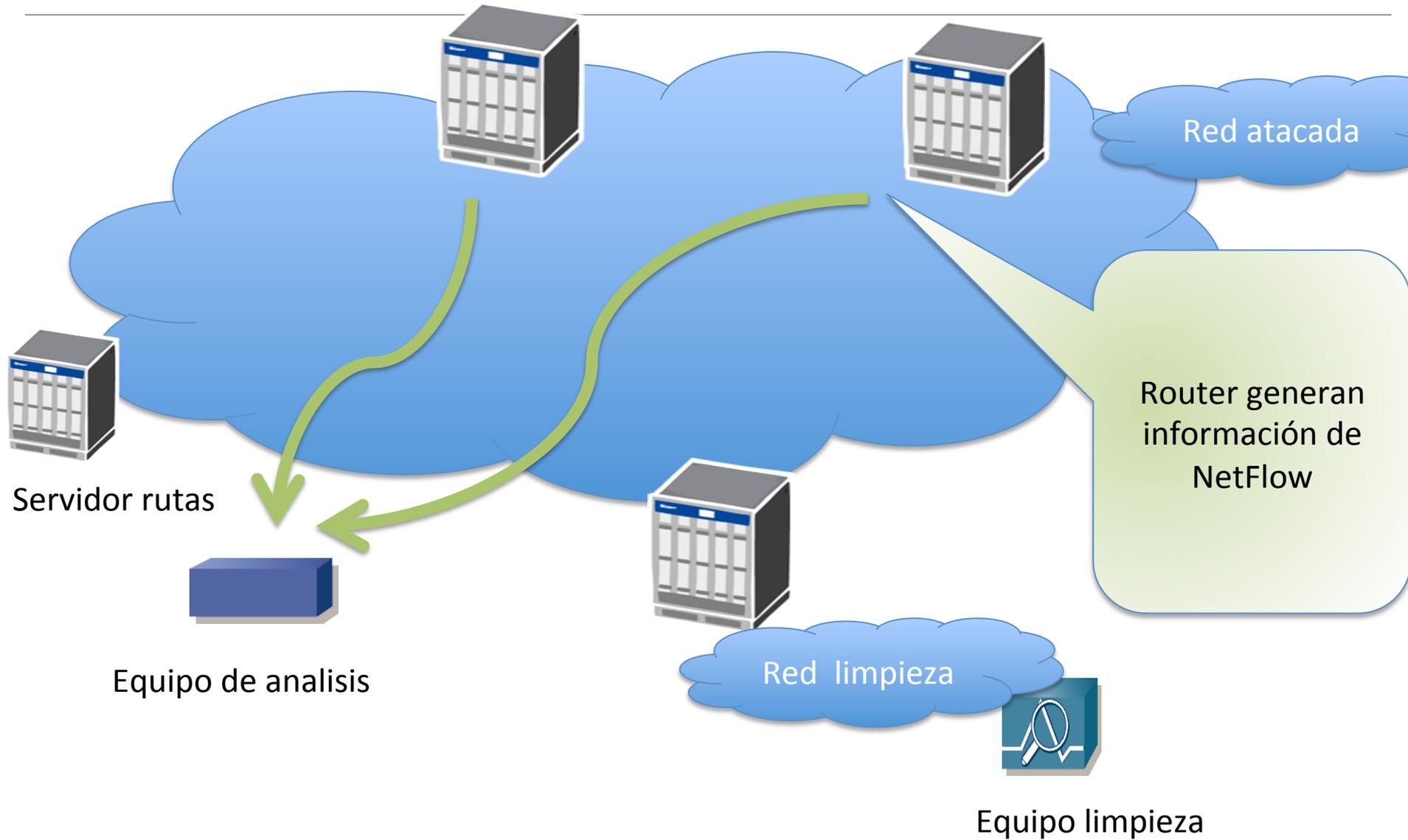


Self IP blocking.

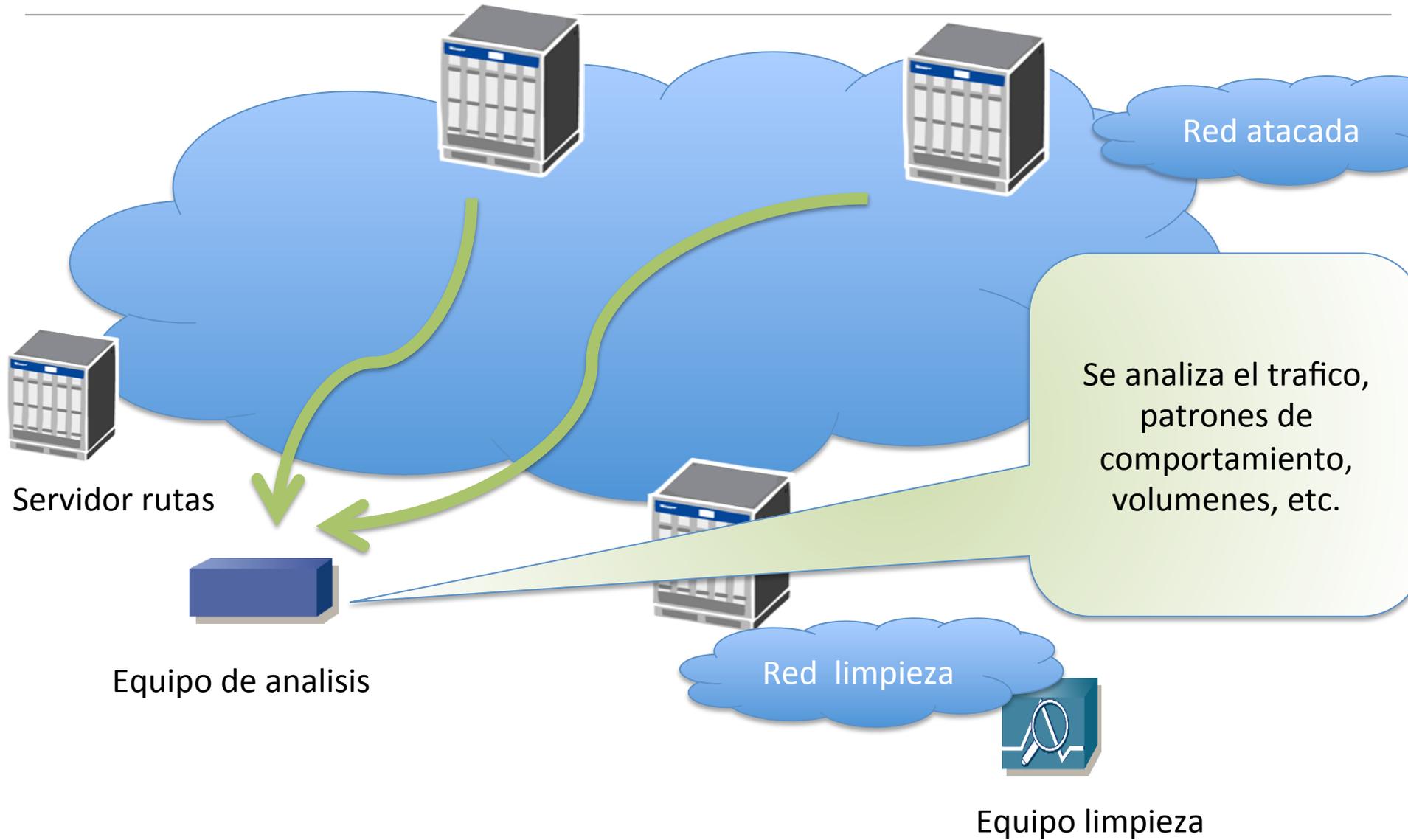
- Por dificultades técnicas el piloto del servicio todavía no esta disponible.
 - Pruebas previstas en diciembre
 - Solicitudes a partir de Febrero
- ¿quién podrá solicitarlo ?

Cualquier institución conectada a RedIRIS

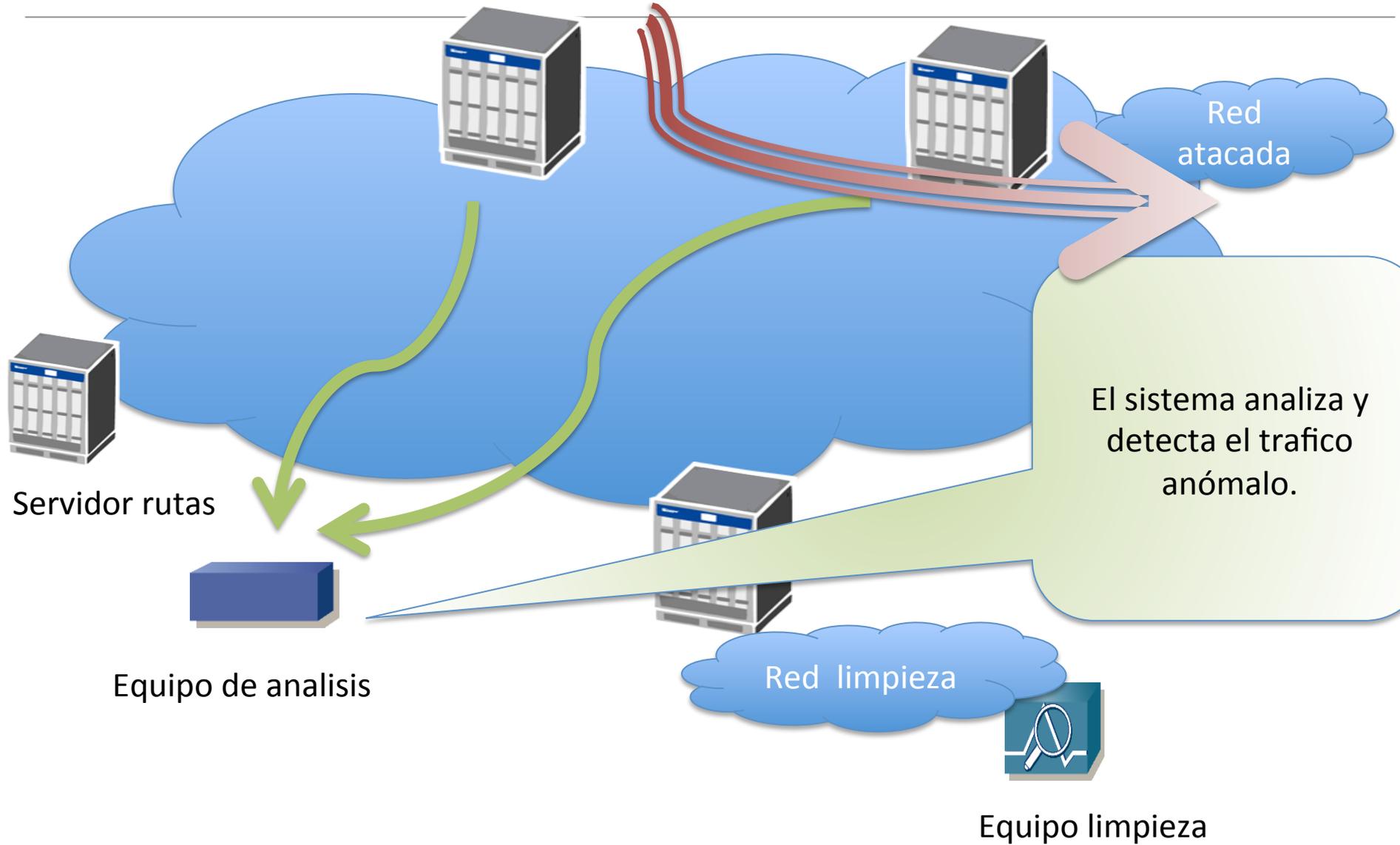
Router Backbone



Router Backbone

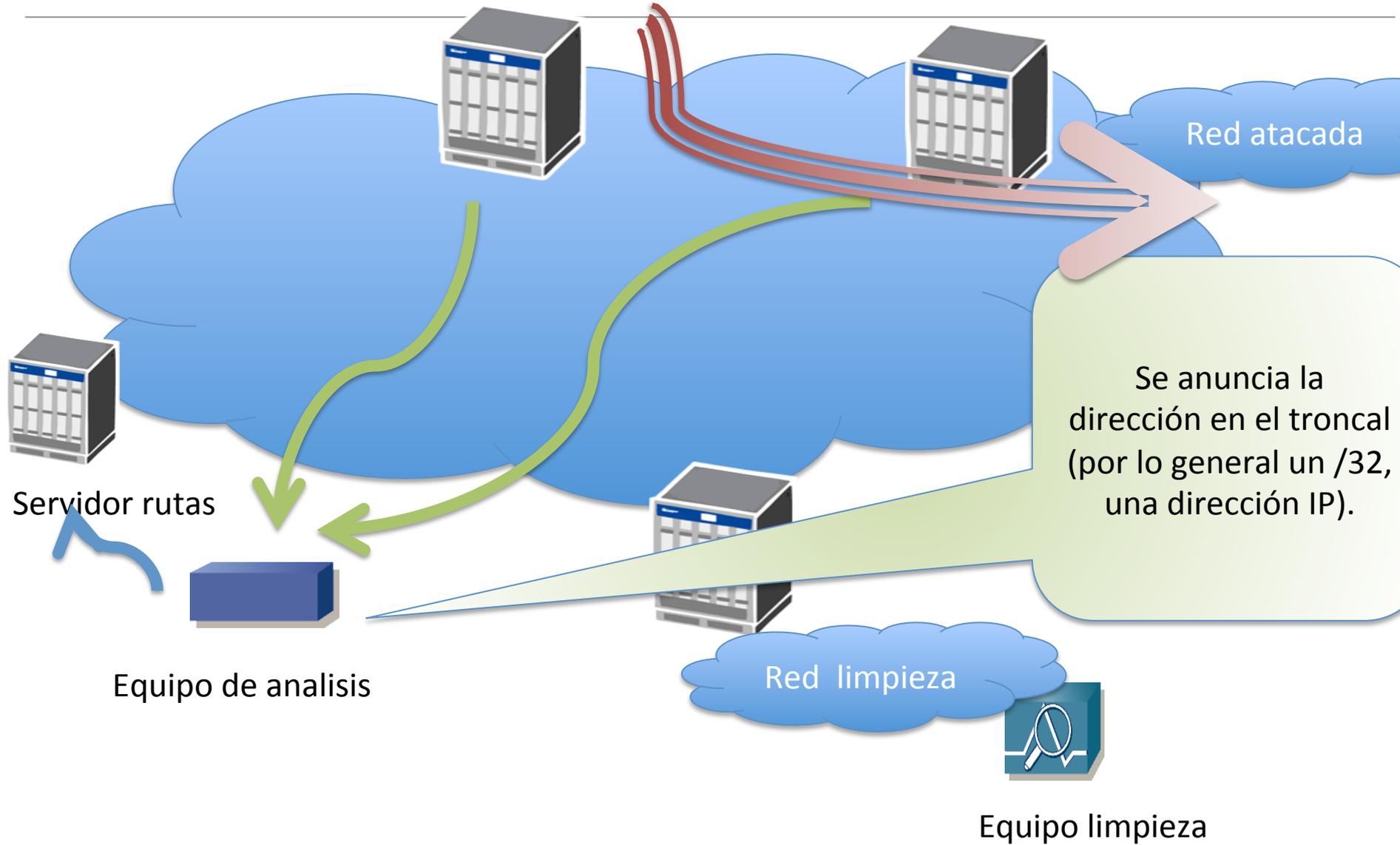


Router Backbone



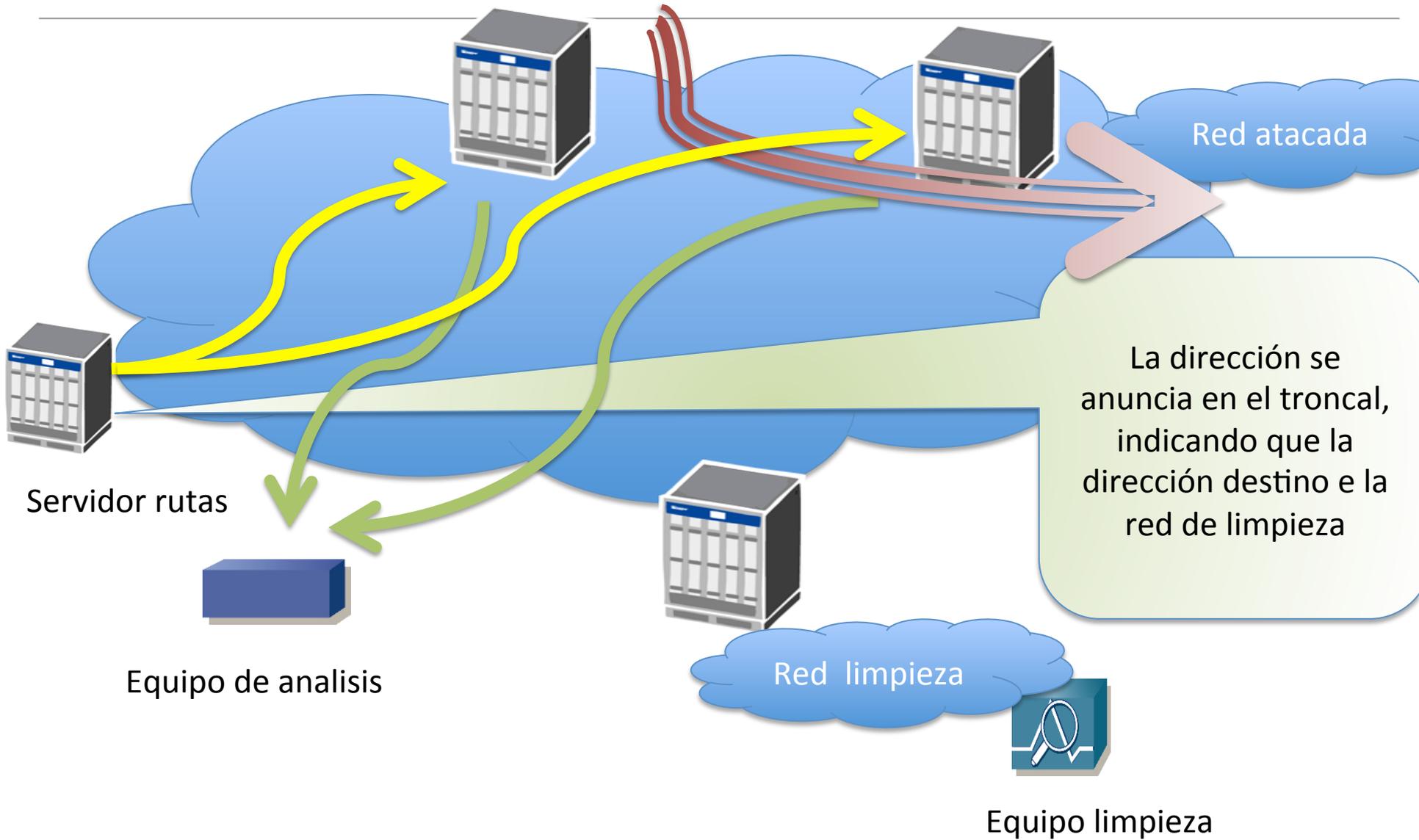
El sistema analiza y detecta el tráfico anómalo.

Router Backbone



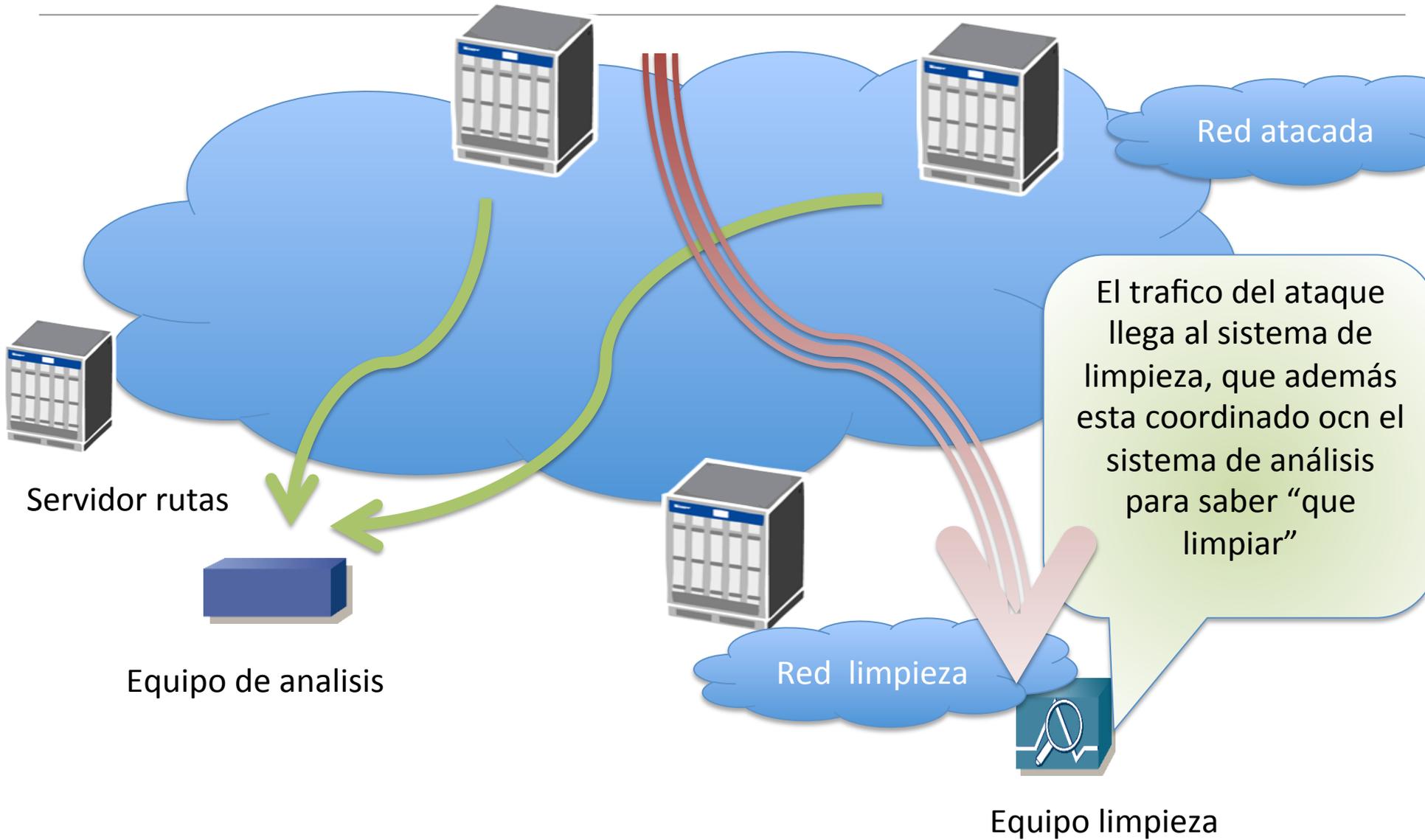
Se anuncia la dirección en el troncal (por lo general un /32, una dirección IP).

Router Backbone



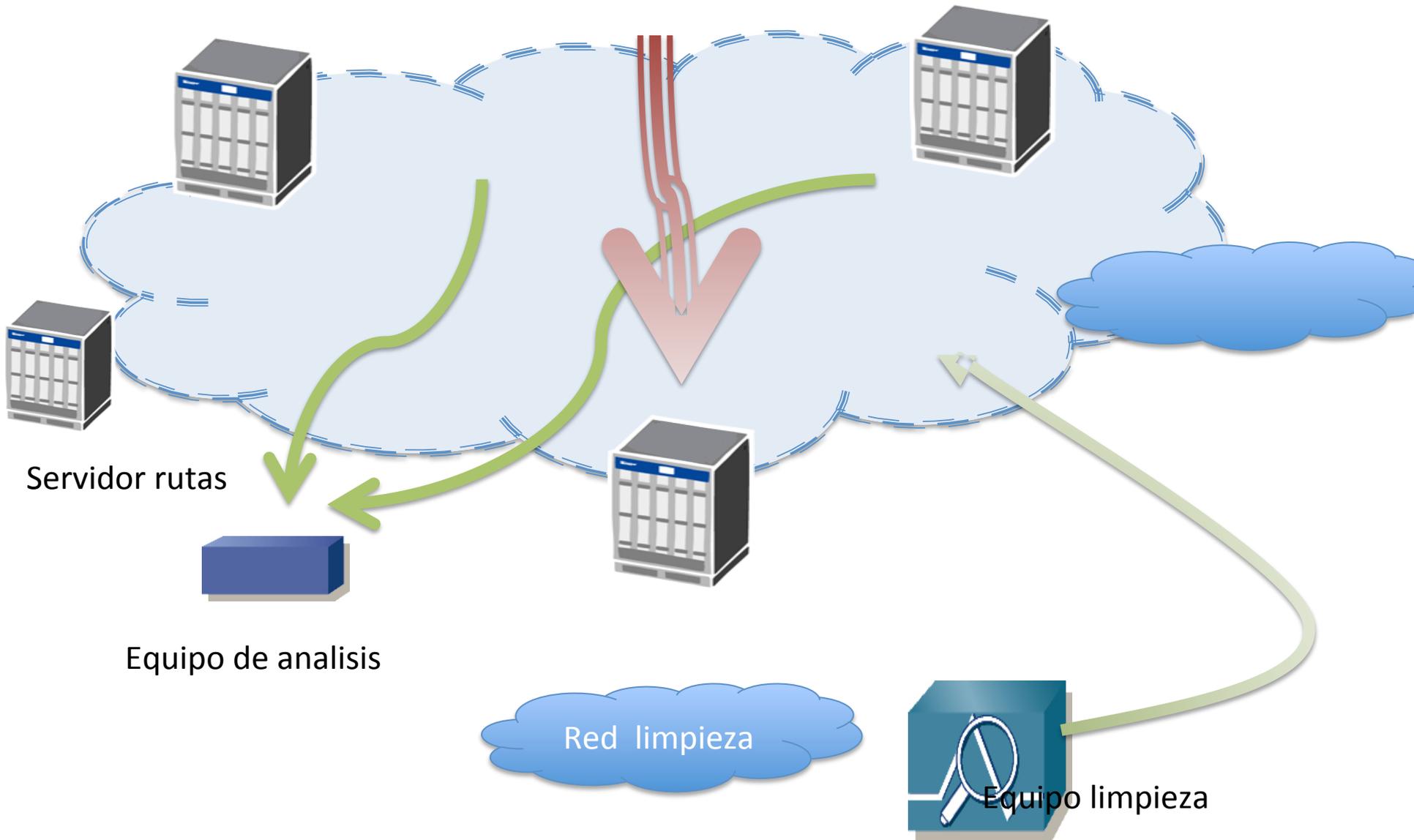
La dirección se anuncia en el troncal, indicando que la dirección destino e la red de limpieza

Router Backbone

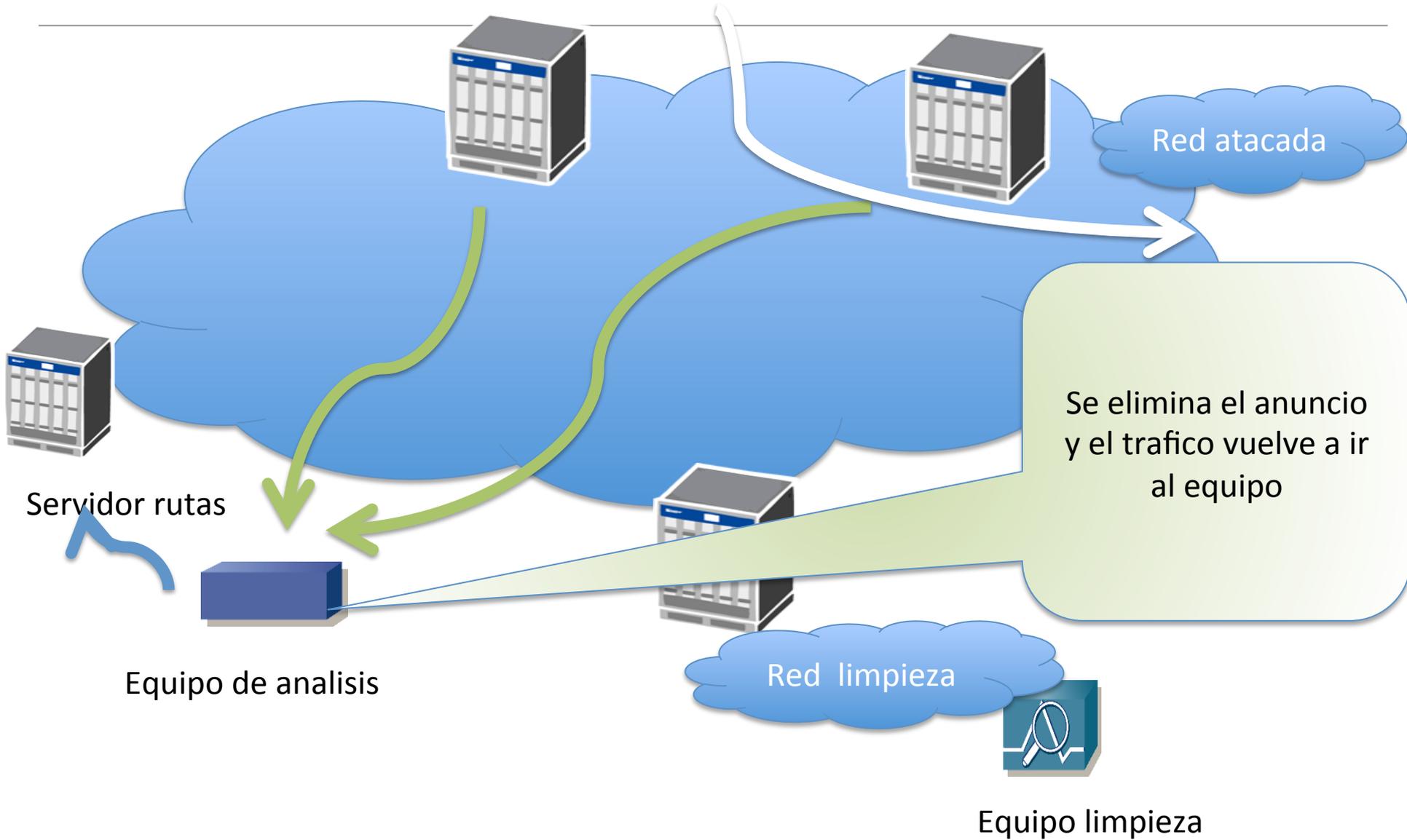


El trafico del ataque llega al sistema de limpieza, que además esta coordinado con el sistema de análisis para saber "que limpiar"

Router Backbone



Router Backbone



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 ilícita 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



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 seguridad



¡Muchas gracias!



Red IRIS

Más de 25 años al servicio de la investigación

