DNS Firewall y RPZ

48º GGTT RedIRIS

Valladolid, 28 de noviembre de 2019

Juan Carlos Rodríguez

Jcarlos.rodriguez@rediris.es

RedIRIS

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

El DNS usado maliciosamente

- La mayoría de las comunicaciones legítimas y no legítimas comienzan con una consulta DNS:
  - Usuarios
  - Servidores
  - Internet de las cosas

- Las fortalezas del DNS se usan de forma maliciosa:
  - muy abierto
  - muy descentralizado
  - muy fiable

DNS Firewall ¿Que es?

El objetivo principal de un firewall DNS es ofrecer protección para:

- bloquear el acceso de los usuarios a sitios web maliciosos
- prevenir ataques de phising
- bloquear comunicaciones desde el interior de nuestra red que usen el DNS como vía de comunicación con el exterior
  - Malware
  - Botnets
- detectar maquinas infectadas en nuestra infraestructura

Ventajas

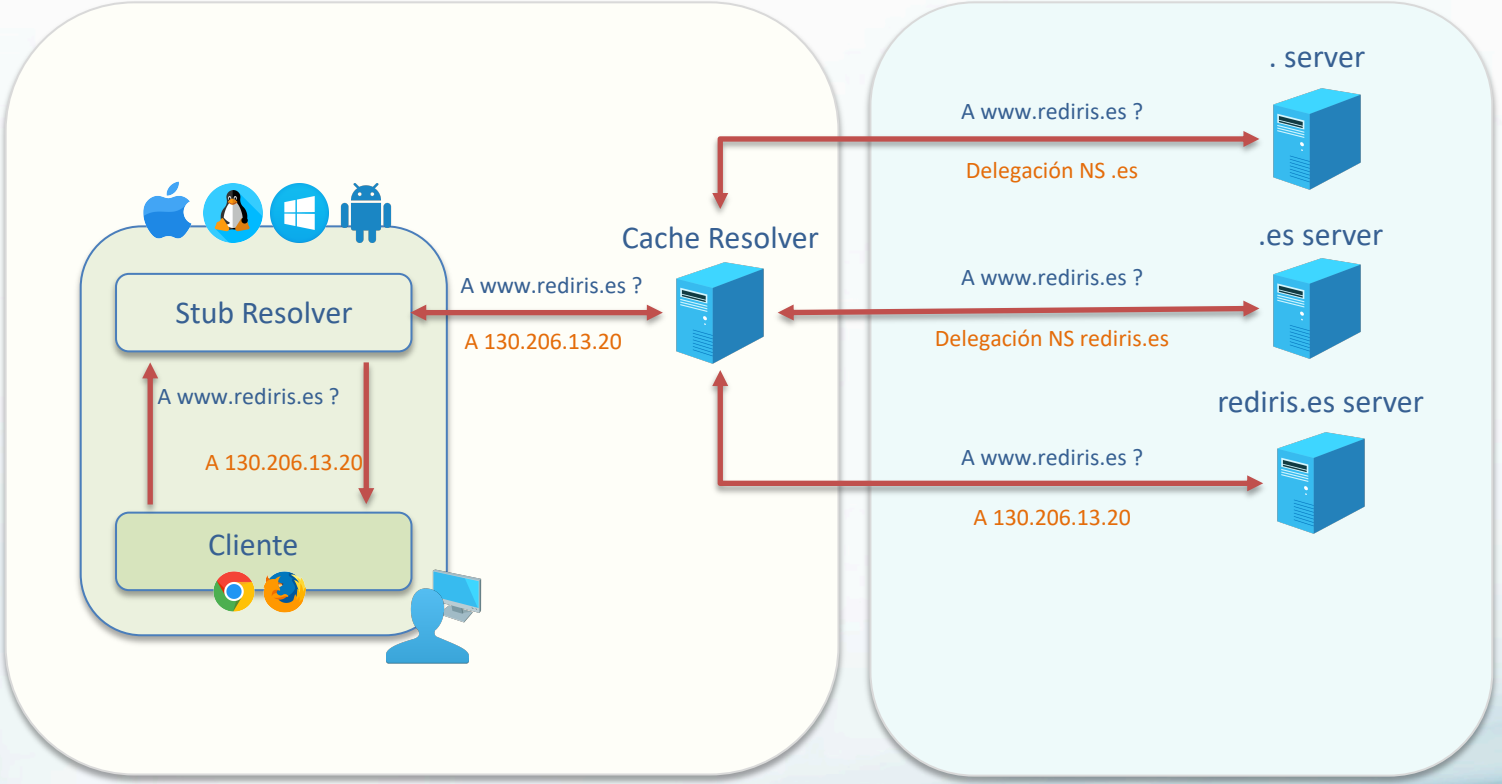
- Rápido de desplegar
- “Fácil” de integrar
- Ofrece protección y visibilidad de lo que ocurre en la red

Tipos de DNS firewall

- Zonas RPZ integradas en los resolvers de las organizaciones
  - Contienen listas de sitios maliciosos y políticas
  - zonas RPZ comerciales de proveedores de seguridad

- Servicios DNS Firewall cloud especializados
  - Integrados en los resolvers más populares
  - Servicios comerciales con funcionalidades adicionales:
    - Logging y estadísticas
    - Políticas de accesos por contenidos
    - API y mensajes personalizados para los usuarios

DNS: funcionamiento normal



RPZ: un poco de historia de la Wikipedia…

- *“The RPZ mechanism was developed by the Internet Systems Consortium led by Paul Vixie as a component of the BIND Domain Name Server DNS.It was first available in BIND release 9.8.1 released 2010, and first publicly announced at Black Hat in July, 2010.”*

- *“The RPZ mechanism is published as an open and vendor-neutral standard for the interchange of DNS Firewall configuration information, allowing other DNS resolution software to implement it.“*

- *“RPZ was developed as a technology to combat the misuse of the DNS by groups and/or persons with malicious intent or other nefarious purposes.”*

https://en.wikipedia.org/wiki/Response_policy_zone

RPZ: configuración

- Soportado en los servidores DNS más habituales:
  - Bind 9.8+, PowerDNS, Knot...
  - Infoblox, EfficientIP, Bluecat...

- Configuradas como zonas especiales:
  - cada dominio tiene una regla y una acción
  - o una acción por defecto para toda la zona

RPZ: reglas

Las reglas RPZ se pueden configurar para buscar por:

- IP Address/Subnet RPZ-IP -> IP contenida en la respuesta
- Hostname/Domain QNAME -> Dominio consultado
- Nameserver Name/Domain RPZ-NSDNAME -> Servidor autoritativo por nombre
- Nameserver Address/Subnet RPZ-NSIP -> Servidor autoritativo por IP
- Client IP RPZ-CLIENT-IP -> Por IP de cliente

RPZ: acciones

Las acciones se pueden definir a nivel de zona o por dominio:

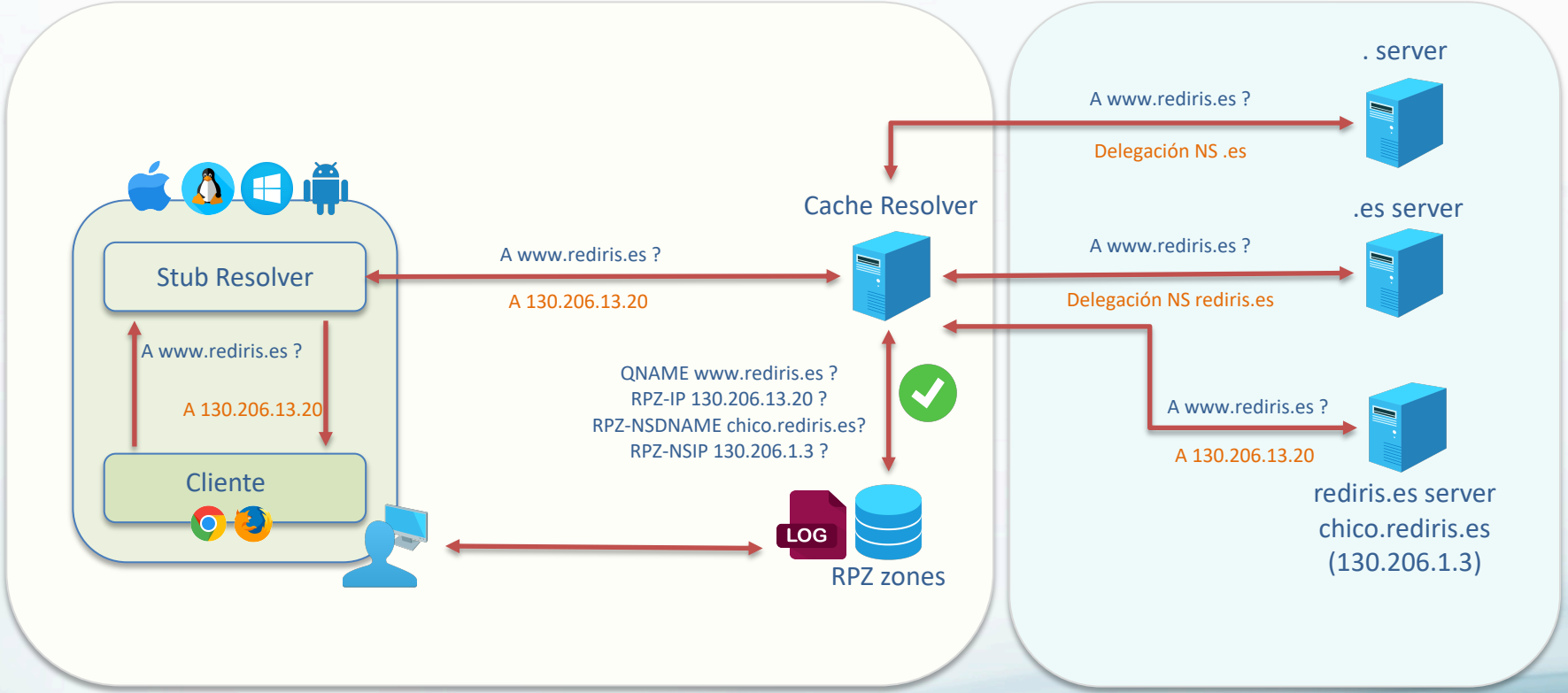
- GIVEN: política por defecto que no sobreescribe la respuesta
- CNAME: se redirige con la respuesta a una pagina web de notificación
- DISABLED: todas las políticas para esta zona se deshabilitan pero se registra la acción
- PASSTHRU: no realiza la acción pero genera un log
- DROP: descarta la petición sin generar respuesta
- TCP-ONLY: fuerza al resolver a realizar la petición por TCP
- NODATA: se responde como que existe el dominio pero no ese tipo de registro
- NXDOMAIN: se responde como que no existe el dominio

RPZ: logs

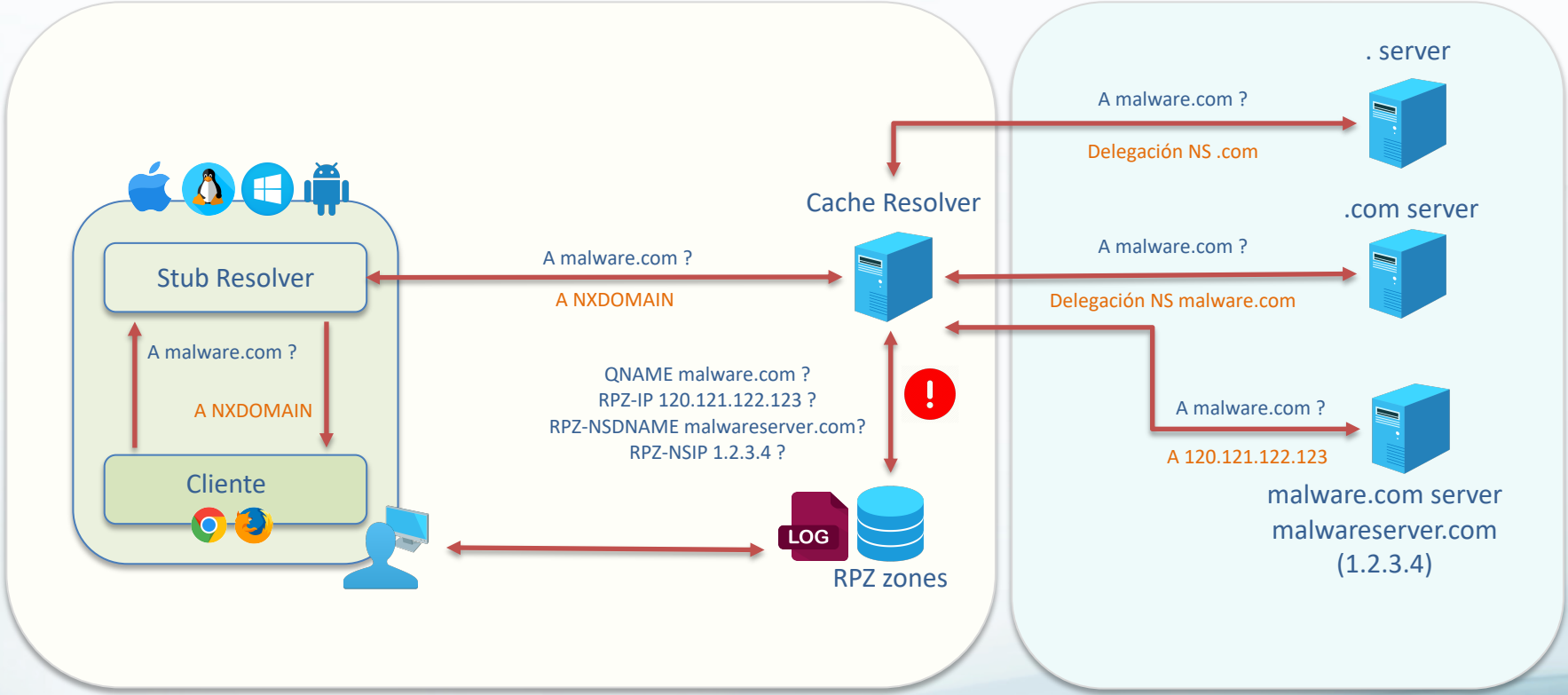
Es tan importante como las acciones en si mismas y sirve para recopilar información de seguridad de nuestra red:

- Máquinas infectadas
- Eventos en marcha
- Integrar y correlacionar con otros orígenes de información

RPZ: funcionamiento: todo OK



RPZ: funcionamiento: dominio filtrado

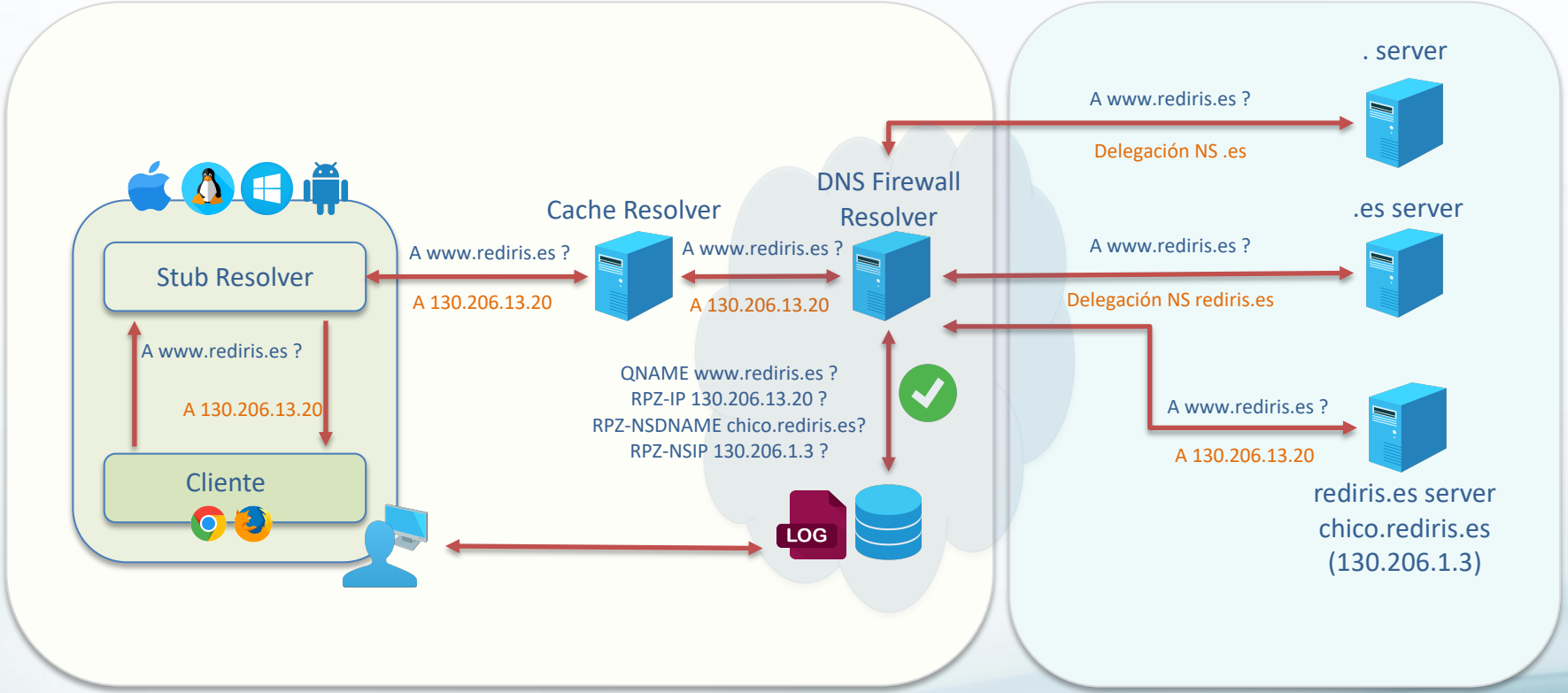


DNS Firewall Cloud

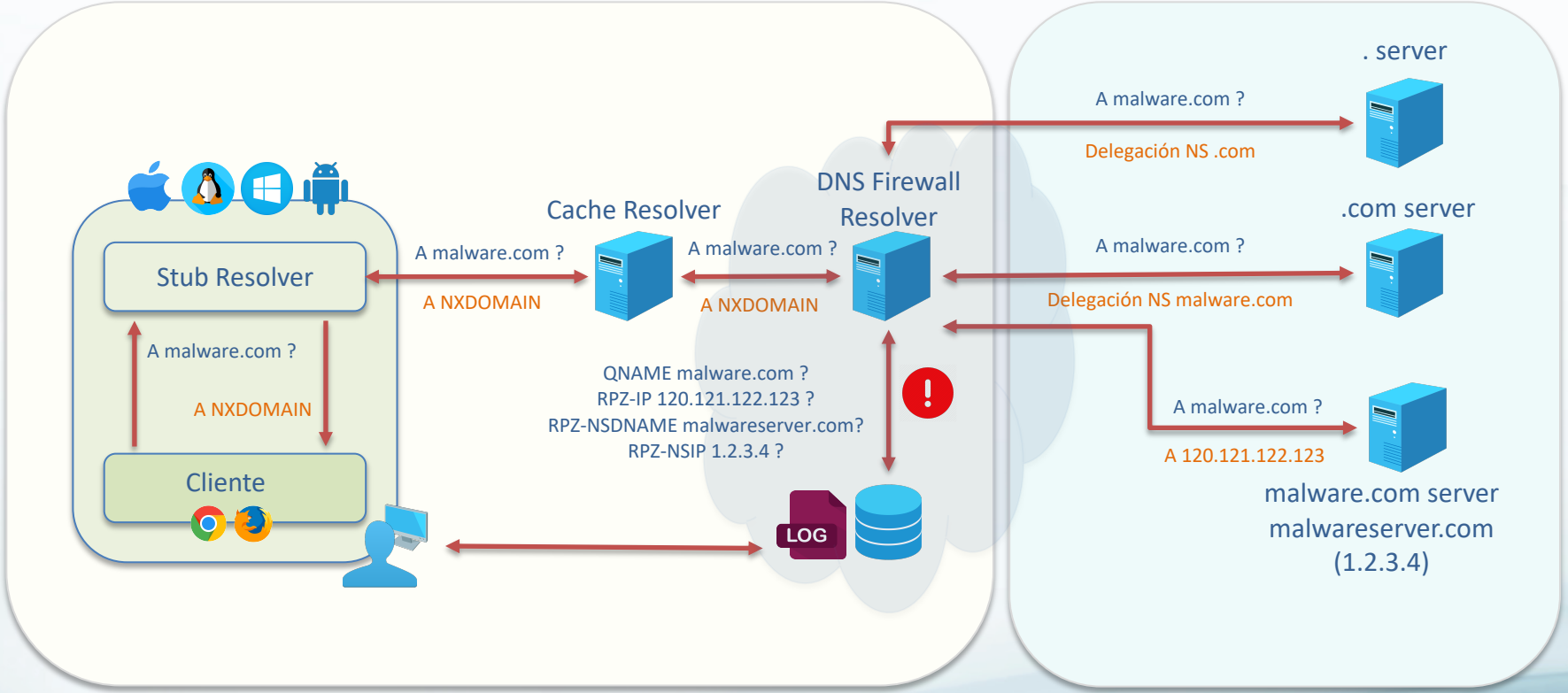
- Resolver “Gratis”
  - Quad9, Google, OpenDNS, Comodo Secure DNS…
  - Se redirigen las queries DNS a la nube del resolver.
  - El proveedor filtra, pero no deja logs, solo aplica acciones tipo RPZ

- Servicios comerciales:
  - Cisco Umbrella, Akamai AnswerX, CIRA D-Zone Firewall…
  - Se redirigen las queries DNS a la nube del resolver.
  - Aplican filtrado por grupos de usuario y contenidos.
  - Generan informes de estadísticas e incidencias.

DNS Firewall Cloud: todo OK



DNS Firewall Cloud: dominio filtrado



Nuevo Servicio RedIRIS

- Nuevo servicio en estudio

- Posibles modelos de servicio
  - REDIRIS como agregador y distribuidor de zonas RPZ
  - REDIRIS como resolver con servicio RPZ integrado
  - REDIRIS como intermediario para servicios DNS Firewall comerciales

- Queremos conocer el interés de la comunidad
  - COMENTARIOS: jcarlos.rodriguez@rediris.es
  - ENCUESTA y DISCUSION: IRIS-DNS@rediris.es

¡Muchas gracias!

Más de 25 años al servicio de la investigación