

HOMELAB · PARTE 01 / 02

EL DNS COMO CORTAFUEGOS

Cómo funciona la resolución de nombres, en qué punto exacto la intercepta AdGuard Home para bloquear rastreadores, qué limitaciones tiene el filtrado por DNS y qué dicen las cifras reales de una red doméstica.

Complemento técnico de la guía «Qué es AdGuard Home»
<https://amstech.dev/guias/adguard-home/01-que-es/>

@ams_tech

ÍNDICE

- 1 Resumen
- 2 El papel del DNS en una conexión
- 3 El mensaje DNS, byte a byte
- 4 Resolución y caché
- 5 El filtrado
- 6 Limitaciones del filtrado por DNS
- 7 Cifras reales de una red doméstica
- 8 Lo que el vídeo simplifica
- 9 Referencias

1. RESUMEN

Antes de abrir cualquier conexión, un dispositivo tiene que traducir un nombre (`api.mixpanel.com`) a una dirección IP. Esa traducción la hace el **DNS** (*Domain Name System*), definido en los RFC 1034 y 1035 [1][2]. AdGuard Home se coloca como resolutor de la red local y, antes de responder, compara cada nombre con listas de filtros. Si el nombre está en ellas, devuelve una dirección nula (`0.0.0.0`) y la conexión nunca llega a producirse.

Este dossier describe el protocolo DNS a nivel de mensaje, con una consulta y una respuesta de bloqueo construidas byte a byte (§3), el proceso de resolución y la caché (§4), el mecanismo de filtrado y sus modos de respuesta (§5), y las limitaciones estructurales del filtrado por nombre: dominios compartidos, DNS cifrado y direcciones IP fijas (§6). En §7 se analizan las cifras del panel de una red doméstica real: 16.849 consultas en 24 horas, de las que se bloquearon 741 (un 4,40 %).

2. EL PAPEL DEL DNS EN UNA CONEXIÓN

Cuando una aplicación quiere hablar con un servidor, el sistema operativo sigue siempre el mismo orden:

1. **Resolución de nombre:** pregunta al DNS por la dirección del servidor.
2. **Conexión:** abre una conexión TCP (o QUIC) con esa dirección.
3. **Cifrado y datos:** negocia TLS y envía la petición HTTP.

El paso 1 es el único que se hace **en claro, por la red local y hacia un servidor que elige la propia red** (el que anuncia el router; lo detalla el dossier de instalación). Por eso es un punto de control tan eficaz: quien responde al DNS decide adónde puede conectarse cada dispositivo, sin instalar nada en él y sin romper el cifrado de los pasos 2 y 3.

Idea clave. El filtrado por DNS no inspecciona el contenido de las conexiones (que va cifrado), sino que impide que lleguen a existir. Es más barato, más privado para el usuario y funciona en cualquier dispositivo, pero solo ve **nombres**: todo lo que no dependa de un nombre propio se le escapa (§6).

3. EL MENSAJE DNS, BYTE A BYTE

Un mensaje DNS tiene una cabecera fija de 12 bytes y cuatro secciones: preguntas, respuestas, autoridad y adicionales [2]. Esta es una consulta real del registro `A` (dirección IPv4) de `api.mixpanel.com`, construida según el RFC 1035:

```

cabecera  1a 2b  01 00  00 01  00 00  00 00  00 00
          ID      flags  QD=1  AN=0   NS=0   AR=0
pregunta  03 61 70 69  08 6d 69 78 70 61 6e 65 6c  03 63 6f 6d  00  00 01  00 01
          3 "api"      8 "mixpanel"          3 "com"      fin A      IN

```

- **ID** (1a2b): número que elige el cliente para emparejar la respuesta con su pregunta.
- **Flags** (0100): solo está activo el bit RD (*recursion desired*): «resuélvemelo tú entero».
- El nombre no viaja con puntos, sino como **etiquetas** precedidas de su longitud (03 api 08 mixpanel 03 com 00).
- **Tipo** 0001 = A y **clase** 0001 = IN (internet).

En total son **34 bytes**; con las cabeceras UDP (8 B) e IPv4 (20 B), **62 bytes** en la red. La respuesta de bloqueo de AdGuard Home repite la pregunta y añade un registro:

```

respuesta c0 0c  00 01  00 01  00 00 00 0a  00 04  00 00 00 00
          nombre A      IN      TTL = 10 s   len=4  0.0.0.0

```

El nombre se comprime con un **puntero** (c00c : «el nombre que empieza en el byte 12», es decir, el de la pregunta), una técnica del propio RFC 1035 para ahorrar espacio. La respuesta completa ocupa **50 bytes** y lleva los flags 8180 : es una respuesta (QR), con recursión disponible (RA) y sin error (RCODE = 0). Para el cliente es una respuesta perfectamente válida; simplemente, la dirección no lleva a ninguna parte.

4. RESOLUCIÓN Y CACHÉ

4.1 LA JERARQUÍA

El espacio de nombres es un árbol: la raíz (.), los dominios de primer nivel (com , org , es ...) y, debajo, los dominios de cada organización. Cada zona tiene **servidores autoritativos**, los que tienen la respuesta oficial [1]. Un **resolvedor recursivo** recorre el árbol desde arriba:

1. Pregunta a un servidor **raíz**, que le remite a los servidores de com .
2. Los de com le remiten a los autoritativos de mixpanel.com .
3. Los autoritativos responden con la dirección.

Hay 13 identidades de servidor raíz (de a a m), replicadas en cientos de ubicaciones con *anycast*: la misma dirección IP anunciada desde muchos sitios, de modo que cada consulta llega al más cercano.

4.2 EL TIEMPO DE VIDA (TTL)

Cada registro lleva un **TTL** (*time to live*): los segundos durante los que se puede guardar en caché [1]. Mientras no caduca, el resolovedor responde de memoria, sin repetir el recorrido. La latencia media que ve el cliente es, aproximadamente,

$$\bar{L} \approx h \cdot L_{\text{caché}} + (1 - h) \cdot L_{\text{upstream}} \approx (1 - h) \cdot L_{\text{upstream}}, \quad (1)$$

donde h es la tasa de acierto de la caché, $L_{\text{caché}} \approx 0$ y L_{upstream} el tiempo que tarda el resolovedor externo. Con un acierto del 60 % y un *upstream* de 20 ms, $\bar{L} \approx 8$ ms: el orden de magnitud de los 9 ms medidos (§7).

4.3 DÓNDE SE COLOCA ADGUARD HOME

AdGuard Home actúa como **resolovedor de reenvío** (*forwarder*): no recorre el árbol él mismo, sino que reenvía las consultas permitidas a un resolovedor recursivo externo (el *upstream*: el de la operadora, Quad9, Cloudflare...) y guarda las respuestas en su caché. El filtrado ocurre **antes** del reenvío: una consulta bloqueada no sale nunca de la red local.

5. EL FILTRADO

5.1 LISTAS Y REGLAS

AdGuard Home carga listas públicas de filtros con dos sintaxis principales [5]:

SINTAXIS	EJEMPLO	SIGNIFICADO
Estilo <i>adblock</i>	<code> api.mixpanel.com^</code>	bloquea el dominio y todos sus subdominios
Estilo <i>hosts</i>	<code>0.0.0.0 api.mixpanel.com</code>	responde esa IP para ese nombre exacto
Excepción	<code>@@ ejemplo.com^</code>	permite un dominio aunque otra regla lo bloquee

Con decenas o cientos de miles de reglas, comparar cada consulta con todas, una a una, sería lento. Por eso las reglas se indexan al cargarlas (por ejemplo, por los fragmentos del dominio), y para cada consulta solo se comprueban las pocas reglas candidatas: el tiempo de decisión apenas depende del tamaño de las listas.

5.2 MODOS DE RESPUESTA

Ante un dominio bloqueado, AdGuard Home puede responder de varias formas [5]:

MODO	RESPUESTA	EFFECTO EN EL CLIENTE
Dirección nula (por defecto para reglas <i>adblock</i>)	0.0.0.0 / ::	la conexión falla al instante, en la propia máquina
NXDOMAIN	«el dominio no existe»	el cliente desiste sin intentar conectar
REFUSED	«me niego a responder»	algunos clientes reintentan con otro servidor
IP personalizada	la que se configure	útil para mostrar una página de aviso

La dirección 0.0.0.0 significa «esta máquina» en muchos sistemas, así que el intento de conexión se resuelve localmente y falla sin generar tráfico. El TTL de las respuestas bloqueadas es configurable: un valor corto hace que, si se desbloquea un dominio, los dispositivos lo noten enseguida.

6. LIMITACIONES DEL FILTRADO POR DNS

6.1 DOMINIOS COMPARTIDOS

El DNS decide por nombre. Si el contenido y la publicidad se sirven desde el mismo dominio (el caso de YouTube, que entrega vídeos y anuncios desde la misma infraestructura), bloquear uno es bloquear el otro. Para eso hace falta un filtro que vea las peticiones completas, dentro del navegador.

6.2 DNS CIFRADO

DNS sobre HTTPS (DoH, RFC 8484 [3]) y **DNS sobre TLS** (DoT, RFC 7858 [4]) cifran las consultas. Es una mejora de privacidad frente a terceros, pero si un navegador o aplicación los usa con **su propio** servidor, sus consultas viajan cifradas por el puerto 443 (o el 853) sin pasar por el resolutor de la red. Las contramedidas habituales son desactivarlo en el cliente, bloquear los nombres de los servidores DoH conocidos o usar el dominio canario `use-application-dns.net`, con el que la red indica a algunos navegadores que no activen DoH por su cuenta.

6.3 DIRECCIONES IP FIJAS

Una aplicación que conecte directamente a una dirección IP escrita en su código no hace ninguna consulta DNS y no puede filtrarse por este método. Es poco habitual en publicidad y analítica (cambiar de IP obligaría a actualizar la aplicación), pero existe.

6.4 FALSOS POSITIVOS

Una lista que incluya un dominio necesario para una función legítima la romperá. El registro de consultas de AdGuard Home permite identificar el dominio responsable y añadir una excepción.

7. CIFRAS REALES DE UNA RED DOMÉSTICA

Datos del panel de mi red, 24 horas consecutivas:

MEDIDA	VALOR	DERIVADO
Consultas totales	16.849	11,7 por minuto
Bloqueadas	741	4,40 % · 30,9 por hora · una cada 117 s de media
Tiempo medio de respuesta	9 ms	compatible con (1) para $h \approx 0,6$

7.1 CÓMO LEER EL 4,40 %

El porcentaje bajo no significa que el efecto sea pequeño: cada consulta bloqueada es una conexión que no se abrió con un servicio de analítica, rastreo o telemetría. Si las consultas fueran independientes, el intervalo de confianza al 95 % de la proporción sería

$$\hat{p} \pm 1,96 \sqrt{\frac{\hat{p}(1 - \hat{p})}{n}} = 4,40 \% \pm 0,31 \%, \quad (2)$$

pero no lo son: los dispositivos repiten las mismas consultas de forma periódica (los informes de telemetría salen a intervalos fijos), así que el intervalo real es más ancho y la cifra hay que leerla como **el valor de ese día en esa red**, no como una constante.

7.2 EL COSTE DEL DNS

Con mensajes de unos 62 bytes en cada sentido, las 16.849 consultas del día suponen unos **2 MB** de tráfico DNS: despreciable. Lo que sí importa es la latencia, porque cada nueva conexión espera a su consulta. Ahí la caché es la clave, y por eso un resolvidor local con caché no ralentiza la red aunque añada un salto.

8. LO QUE EL VÍDEO SIMPLIFICA

EN EL VÍDEO	CON PRECISIÓN
«Te espían 741 veces»	741 consultas a dominios de analítica, rastreo y telemetría según las listas activas; no todas transmiten datos personales
«No le da la dirección»	Le da una dirección nula (0.0.0.0) o un «no existe», según el modo
«Filtra todo internet en tu casa»	Filtra las consultas DNS de los dispositivos que lo usan como resolvidor; no ve el contenido ni el tráfico que no pase por DNS
«Nunca se carga»	Nunca se establece la conexión, salvo que el dispositivo use DNS cifrado propio o IPs fijas

9. REFERENCIAS

- [1] P. Mockapetris. *RFC 1034: Domain Names — Concepts and Facilities*. IETF, 1987. <https://www.rfc-editor.org/rfc/rfc1034>
- [2] P. Mockapetris. *RFC 1035: Domain Names — Implementation and Specification*. IETF, 1987. <https://www.rfc-editor.org/rfc/rfc1035>
- [3] P. Hoffman, P. McManus. *RFC 8484: DNS Queries over HTTPS (DoH)*. IETF, 2018. <https://www.rfc-editor.org/rfc/rfc8484>
- [4] Z. Hu et al. *RFC 7858: Specification for DNS over Transport Layer Security (TLS)*. IETF, 2016. <https://www.rfc-editor.org/rfc/rfc7858>
- [5] AdGuard. *AdGuard Home: documentación (configuración, sintaxis de filtros y modos de bloqueo)*. <https://github.com/AdguardTeam/AdGuardHome/wiki>
- [6] P. Hoffman, A. Sullivan, K. Fujiwara. *RFC 9499: DNS Terminology*. IETF, 2024. <https://www.rfc-editor.org/rfc/rfc9499>

Los mensajes de §3 y las cifras derivadas de §7 se han calculado con un script propio. Las cifras del panel son de mi red y se muestran sin IPs ni nombres de dispositivos.