

# Servicio De Red IRIS

---

CISCO UMBRELLA

## Que es un DNS Firewall

---

Es la primera barrera de protección, ya que la mayoría de las comunicaciones, legítimas o no, de todos los elementos de nuestras redes comienzan con una consulta DNS.

Una herramienta de seguridad, adicional y complementaria a los Firewall y otras herramientas de inspección de tráfico, enfocado al tráfico DNS.

Redirige o bloquea el acceso de los usuarios finales a sitios maliciosos.

Ventajas:

1. “Rápido” de desplegar
2. “Fácil” de integrar
3. Ofrece protección y visibilidad de lo que ocurre en la red



Red IRIS



# Que es un DNS Firewall: Arquitecturas

---

Zonas RPZ integradas en los resolvers de las organizaciones:

- Contienen listas de sitios maliciosos y políticas
- Zonas RPZ comerciales de proveedores de seguridad (Free-€-€€)
- Reactivas (listas actualizadas a posteriori)

Servicios DNS Firewall cloud especializados

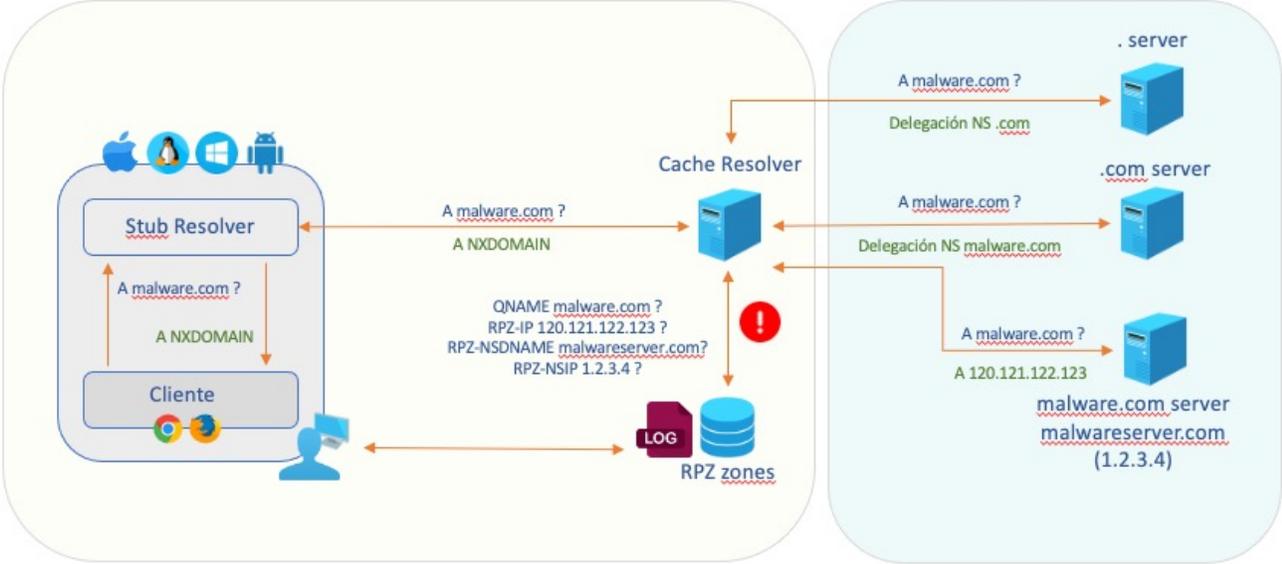
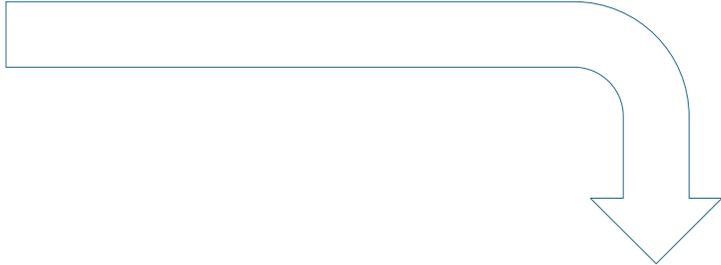
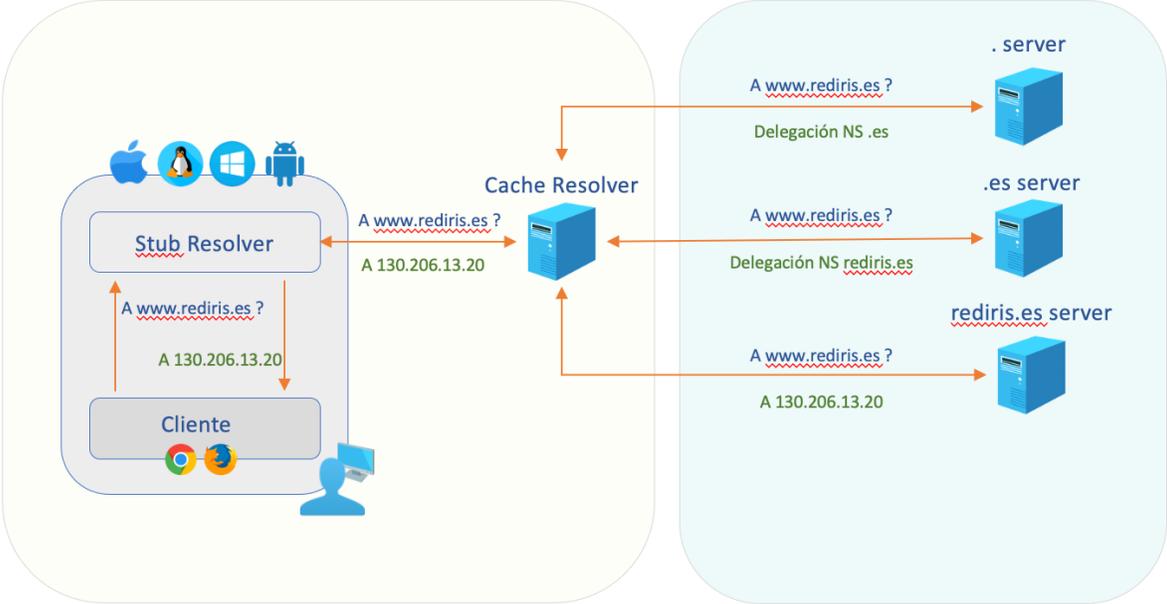
- Integrados en los resolvers más populares (Google, Cloudflare, Quad9...) (Free)
- Servicios comerciales con funcionalidades adicionales (€€€):
  - Logging y estadísticas
  - Políticas de accesos por contenidos
  - API y mensajes personalizados para los usuarios
  - Proactivas (heurística, sandboxing, machine learning, etc)



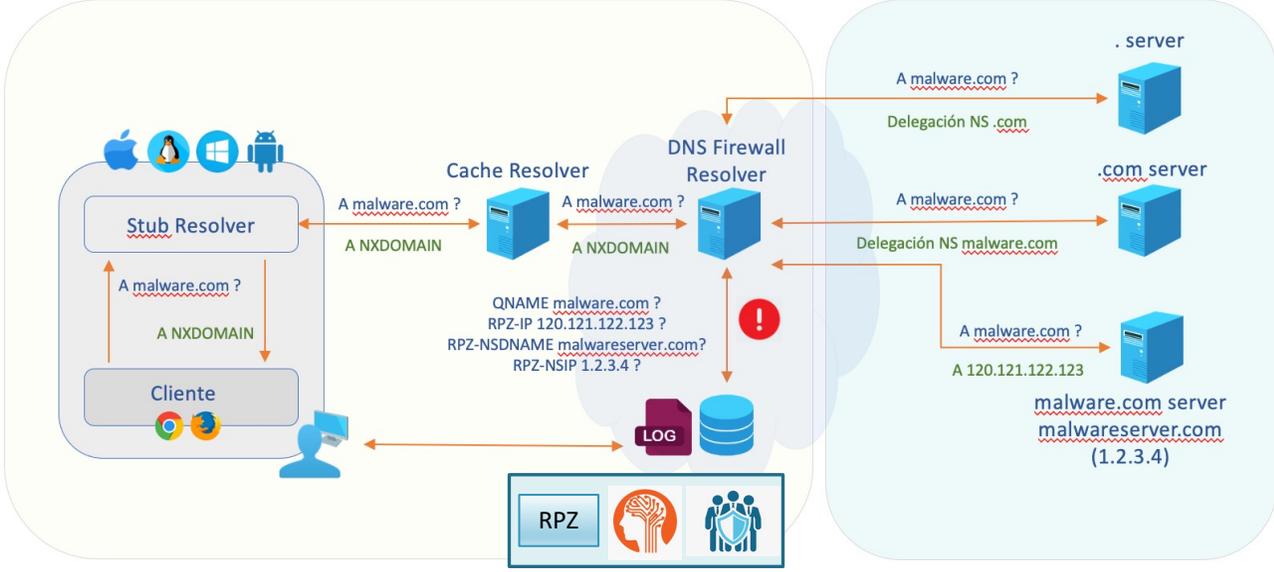
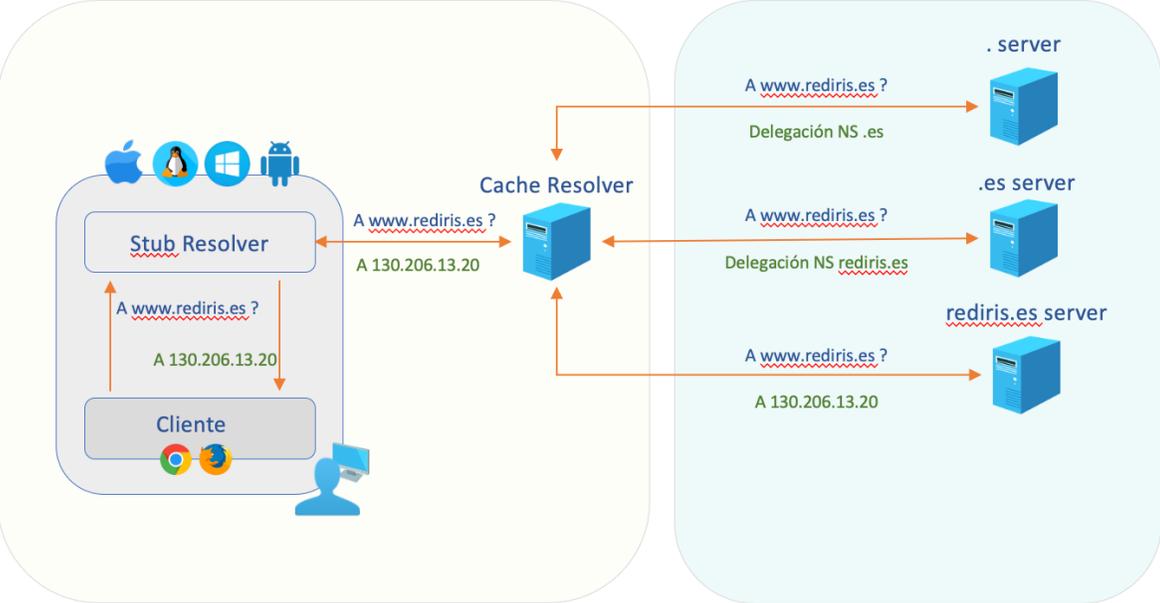
Red IRIS



# DNS Firewall: Protección RPZ



# DNS Firewall: Protección Servicio Cloud



# Datos de la licitación

---

## 088/21-RI “SERVICIO DE DNS FIREWALL DE REDIRIS”

- Duración: 24 meses periodo inicial (desde 23/05/2022 hasta 23/05/2024) + 12 meses de prórroga (hasta 23/05/2025)
- Financiado mediante Fondo de Recuperación Next Generation EU.
- Requisitos:
  - Plataforma tecnológica de protección DNS. Cloud y multitenant. 1.900.000 licencias entre alumnado + PAS + PDI +PI
  - Equipo de administración y gestión de la plataforma 8x5. 1 medio personal.
  - Equipo de Gestión y resolución de incidencias. 24x7
- Importes de Adjudicación
  - Importe total ofertado (con impuestos) 1.780.754,28 EUR (2 años, 1 año adicional opcional)
  - Adjudicado a CSA junto a Cisco Umbrella



Red IRIS



# Servicio DNS Firewall en RedIRIS

---

## Plataforma CISCO UMBRELLA:

- Arquitectura cloud Anycast para garantizar la mayor disponibilidad posible y resiliencia ante fallos, con más de 30 nodos y alta dispersión geográfica.
- Servicio multitenant, de forma que cada institución puede personalizar el funcionamiento del servicio y obtener sus propias estadísticas de uso y alertas.
- Despliegue sencillo, ya que sólo es necesario reencaminar el tráfico DNS hacia los resolver del servicio.

## Servicio de administración y soporte:

- Servicio de administración en modalidad 8x5 para consultas, asesoría y altas.

Contacto vía correo electrónico a [dnsfirewall@rediris.es](mailto:dnsfirewall@rediris.es)

- Atención de incidencias 24x7 para incidencias:
  - Contacto vía correo electrónico a [dnsfirewall@rediris.es](mailto:dnsfirewall@rediris.es) añadiendo la palabra incidencia en el asunto para mejor atención.
  - A través de contacto telefónica (34 607 359 278) indicando el PIN del servicio definido al realizar el alta en el servicio.



Red IRIS



# Qué es CISCO UMBRELLA

---

- Servicio en la nube, el despliegue básico no requiere instalación de software ni hardware.
  - Instalaciones avanzadas permiten integración con directorio activo e instalación de agentes en dispositivos.
- Mediante patrones de actividad en Internet, Umbrella puede descubrir ataques y bloquear sitios maliciosos.
  - Usa modelos estadísticos y machine learning propios.
  - Dispone de un equipo humano de investigadores.
- Se integra con SIEMs y/o sistemas de syslog.
- Mediante API se pueden cargar listas negras para realizar bloqueos de sitios maliciosos.
- Se ha adquirido el paquete: DNS Security for Education.



Red IRIS



# Arquitectura

---

Las direcciones de **DNS de UMBRELLA** son:

- IPv4:208.67.220.220 and 208.67.222.222
- IPv6:2620:119:35::35 and 2620:119:53::53

Hay varios escenarios para integrar **CISCO UMBRELLA** en nuestra red:

- Escenario 1: Hacer forwarding de nuestro resolver a Umbrella.
- Escenario 2: Desplegar Agentes.
- Escenario 3: Instalación on premise.

Funcionamiento resumido

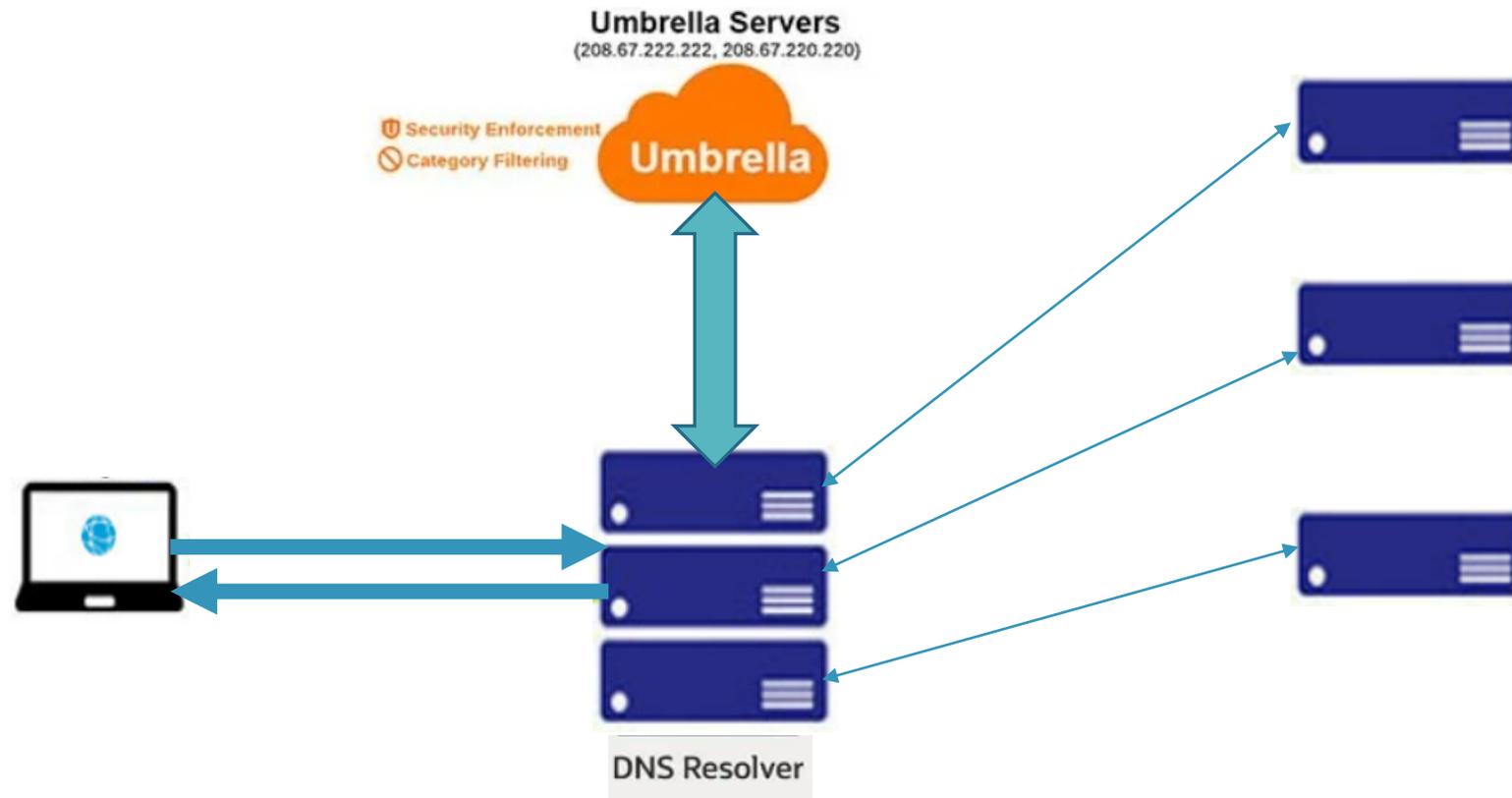
- Definición de políticas de categorización por temática o seguridad
- Definición de acciones (página de bloqueo, no responder, sólo registrar...)
- Aplicar a redes, máquinas o perfiles de AD



Red IRIS



## Escenario 1: Hacer forwarding de nuestro resolver a Umbrella



- Forwarding desde el Resolver.
- Perdemos el seguimiento del usuario que hace la petición. Con excepciones.



Red IRIS



# Escenario 1: Cómo hacer el forwarding:

---

## DNS BIND:

- *# Configuración para DNS Firewall (servidores de Umbrella)*  
*# Forwarding de las peticiones a las IPs de Umbrella*

```
forwarders {  
    208.67.220.220;  
    208.67.222.222;  
    2620:119:35::35;  
    2620:119:53::53;  
};  
  
# Primero pregunta a los servidores de forwarding,  
# si no lo consigue, lo resuelve normalmente.  
forward first;
```

## PowerDNS:

- (1) En el fichero de configuración `recursor.conf` (generalmente `/etc/pdns-recursor/recursor.conf`) de `pdns-recursor` incluir las opciones:  

```
# Configuración para DNS Firewall (servidores de Umbrella)  
# Reenvío de peticiones a servidores recursivos de Umbrella  
forward-zones-recurse=. =208.67.220.220;208.67.222.222;2620:119:35::35;2620:119:53::53
```
- (2) Reiniciar el servidor para aplicar la configuración.  

```
$ systemctl restart pdns-recursor
```



# Escenario 1: Guía de primeros pasos y configuración

## Infoblox, Efficientip, Microsoft...

- Guía de configuración publicada en <https://www.rediris.es/dnsfirewall>

ayuda\_dnsfir...

ayuda\_dnsfirewall.pdf

```
ifconfig_lo0_alias53="inet 127.0.1.53 netmask 255.0.0.0"
```

6) Acceder a la consola de gestión de SOLIDServer. Ir a (1) DNS (2) Servers (3) Seleccionar el servidor DNS Smart. Hacer click en el botón derecho y seleccionar "Properties".

7) Hacer click en el botón de "EDIT" en la sección de "FORWARDING".

12

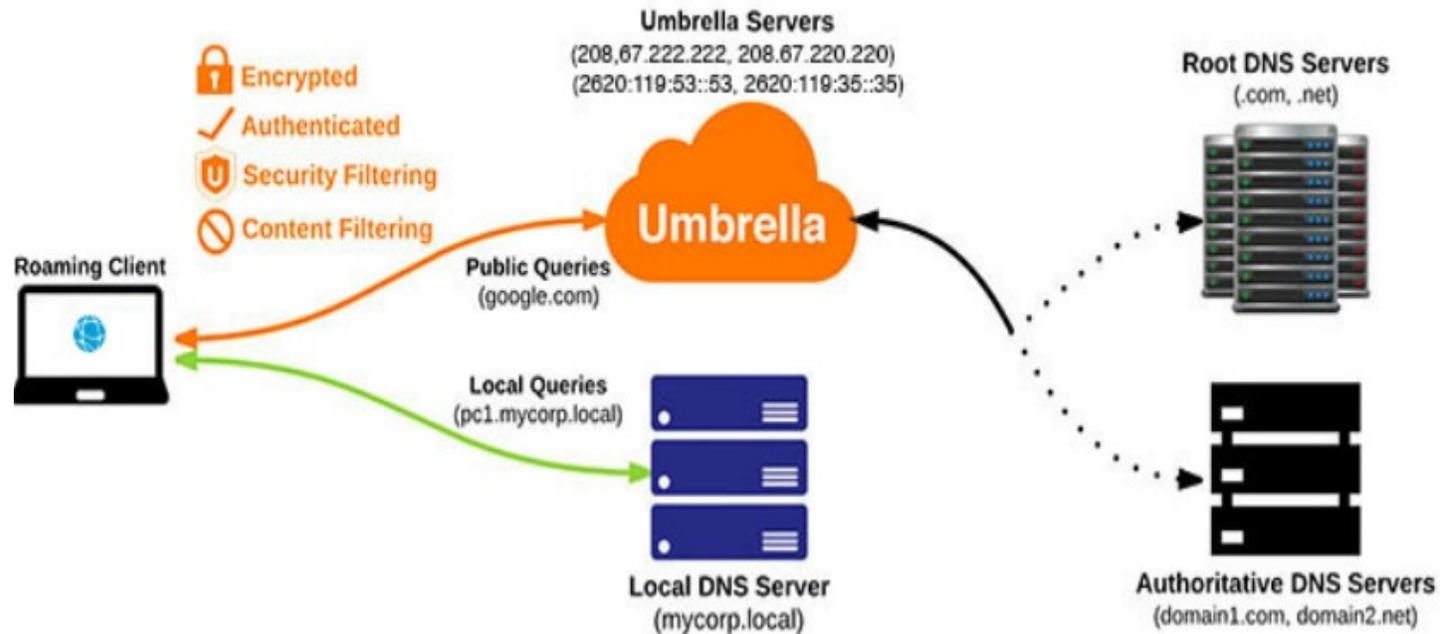
RedIRIS DNS FIREWALL



RedIRIS



## Escenario 2: Desplegar Agentes



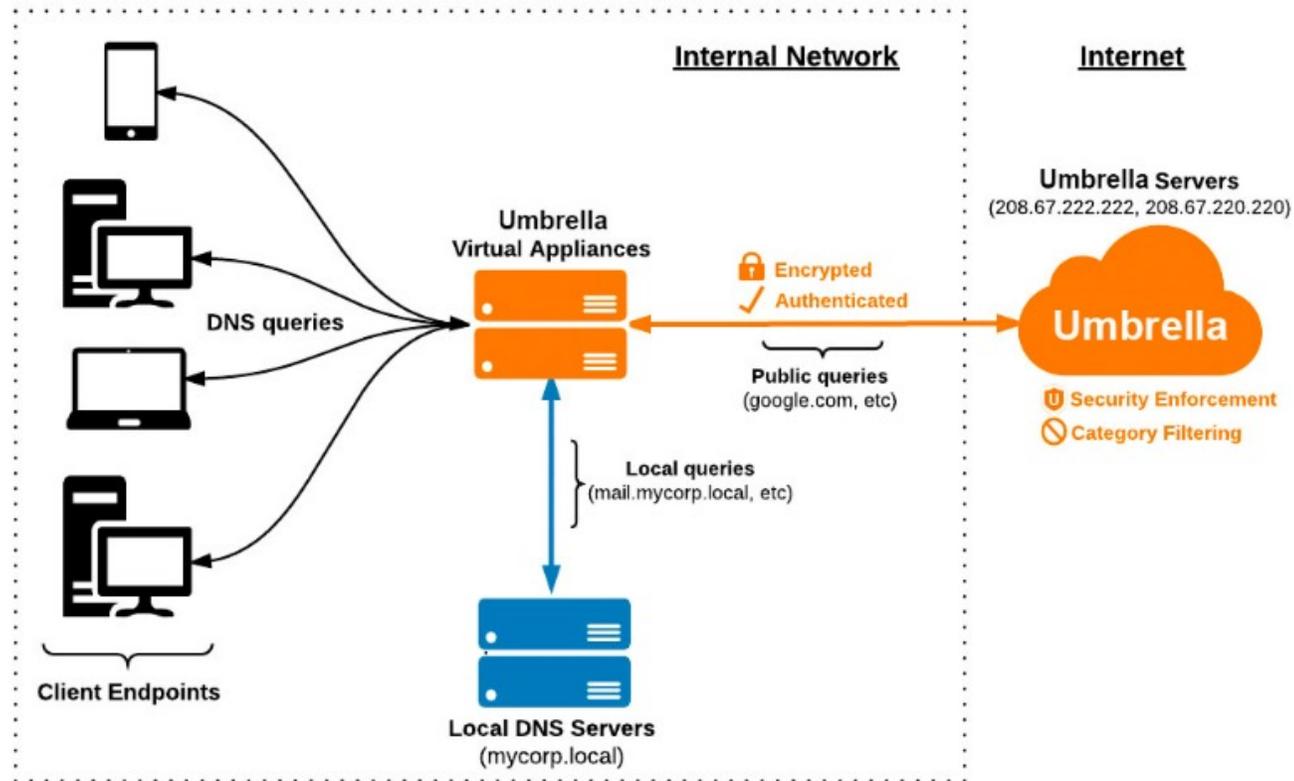
- Para móviles y PCs en roaming, se redirigen directamente las consultas a Umbrella desde cualquier ubicación
- Documentación oficial de la instalación: [Download and Install the Roaming Client \(umbrella.com\)](https://umbrella.com/docs/Download-and-Install-the-Roaming-Client)
- Con este sistema tenemos identificados lo equipos que hacen las peticiones.



Red IRIS



## Escenario 3: Instalación on premise



- Dos máquinas virtuales, para generar alta disponibilidad:
- Permite tener visibilidad de las IP internas de las consultas
- Permite aplicar políticas en base a atributos de AD



Red IRIS



## Escenario 3: Instalación on premise

---

### AD Connector:

Es un elemento añadido a la arquitectura con VA. Instalando este elemento se reporta a la nube toda la información del usuario final.

### Despliegue:

- Requisitos:
  - Una máquina virtual con Windows para desplegar el AD Conector.
  - Usuario con permisos específicos de administración. Se puede dar de alta directamente en el AD o lanzar el script para que lo genere.
- Una vez finalizada la instalación, el AD le reporta periódicamente una lista de usuarios al AD Connector. Cuando las VA reciban una petición DNS, solicitarán la información del usuario que ha realizado dicha petición al AD Connector.

Las VA encaminaran la petición a la nube con toda la información de máquina y de usuario.



Red IRIS



## El correo, caso excepcional

---

La recomendación de CISCO es **no dirigir las peticiones DNS del correo** hacia Cisco UMBRELLA ya que podría interferir con otros procesos de seguridad como el filtrado antispam.



Red IRIS



# Configuración Inicial del tenant

---

Hay que activar el **2FA** y la **zona horaria**.

- Este paso lo tienen que realizar todos los administradores cuando se les entregue la cuenta, de su propio perfil.

Configuración centralizada:

- **Modo transparente**. (se registran todas las consultas pero no hay bloqueos). Se entrega el tenant con esta configuración se puede solicitar cambiar a las siguientes:
- Modo seguridad básico (malware, phishing, C&C, cryptomining, Tunneling)
- Modo seguridad alto. (básico + new and Dynamic domains, potentially harmful)

Las redes están configuradas. Se pueden hacer subnetting.

El administrador tiene control total sobre el tenant. Puede crear y aplicar nuevas políticas, listas blancas/negras, crear usuarios, etc.



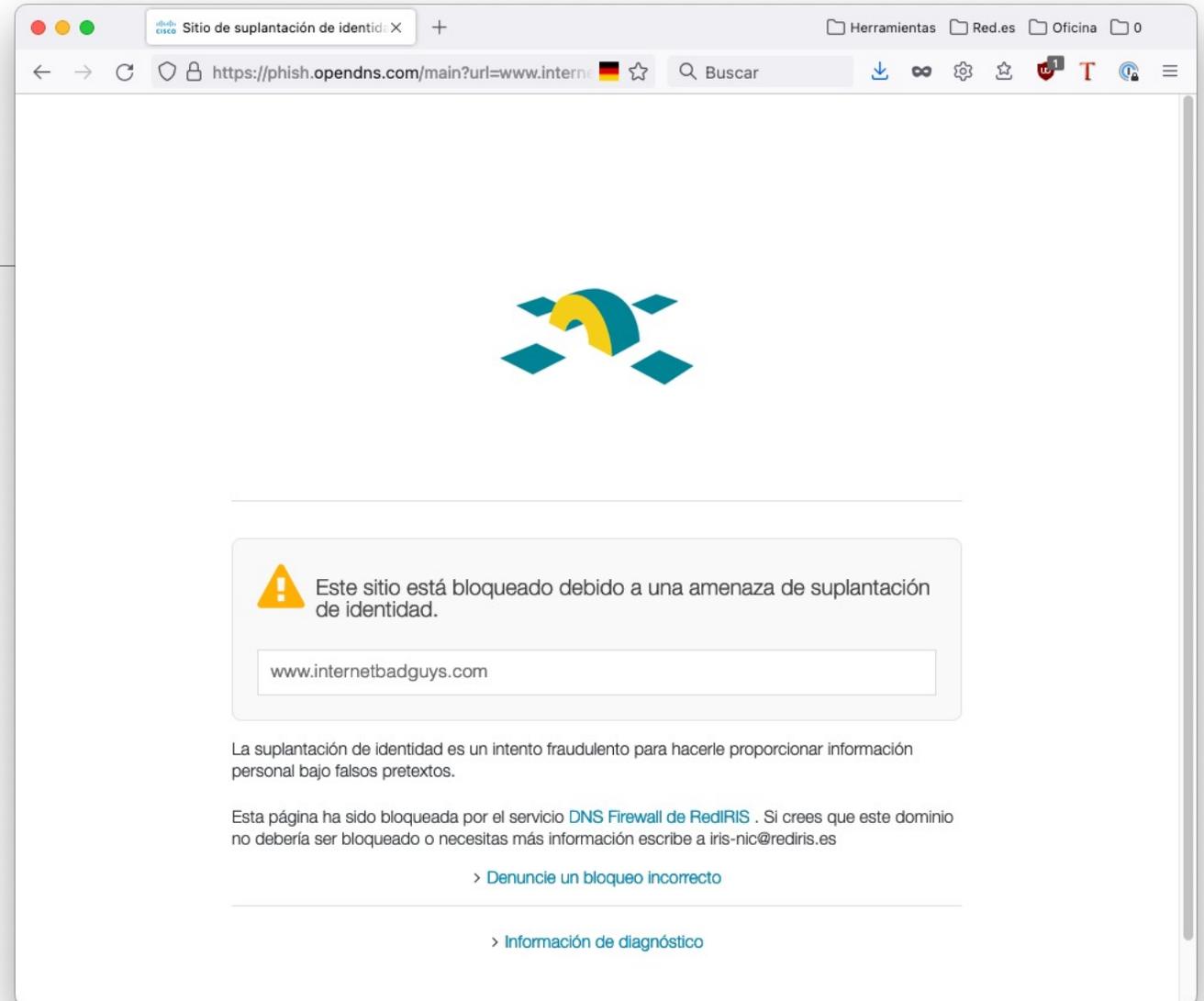
Red IRIS



# Configuración Inicial del tenant

Varios comportamientos:

- Redirección web
  - pagina personalizable
  - a URL externa
- No responder
- Respuesta no existe el dominio...



RedIRIS



# Aspecto del tenant

The screenshot shows the Cisco Umbrella tenant overview dashboard. On the left is a navigation sidebar with the following items: Overview, Deployments, Policies, Reporting, Investigate, Admin, a user profile for Juan Carlos Rodriguez (RedIRIS), and a 'Need Help?' section with links for 24/7 Phone Support, Click Here, Service Status (All services are operational), Documentation, Support Platform, Learning Center, Cisco Online Privacy Statement, Terms Of Service, and © Cisco Systems. The main content area is titled 'Overview' and includes a 'Schedule' button and a 'LAST 24 HOURS' filter. Below this is a 'Messages' section with three rows: 'Malware: 30 requests blocked in the last 24 hours', 'Botnet: 0 requests blocked in the last 24 hours', and 'Cryptomining: 0 requests blocked in the last 24 hours'. The 'Deployment Health' section features three gauges: 'Active Networks' at 12% (7/59 Active), 'Active Roaming Clients' at 0% (0/0 Active), and 'Active Virtual Appliances' at 0% (0/0 Active). The 'Network Breakdown' section has a 'See All Security Events' checkbox and three line charts: 'Total Requests' (464.8K Total, -14% vs. previous 24 hours), 'Total Blocks' (54 Total, +135% vs. previous 24 hours), and 'Security Blocks' (54 Total, +135% vs. previous 24 hours). The bottom of the dashboard shows the Cisco logo, 'SECURE X Home', and utility icons for 'Enrich...', search, settings, help, and a plus sign.



RedIRIS



# Aspecto del tenant

The screenshot displays the Cisco Umbrella Security Activity reporting interface. On the left is a navigation sidebar with categories like Overview, Deployments, Policies, Reporting, Core Reports, Activity Search, App Discovery, Top Threats, Additional Reports, and Management. The main content area is titled 'Security Activity' and includes a search bar, a bar chart for 'All Security Activity (Last 24 Hours)', and a list of events. The bar chart shows activity peaks around 2:00 am and 10:00 pm. The event list shows two blocked items: a phishing attempt from 'www.internetbadguys.com' and a malware event from '195-154-42-43.rev.poneyt...'. The interface also features filters for time and event type, and a 'RESPONSE' section at the bottom.

**Cisco Umbrella** Reporting / Core Reports  
**Security Activity** Schedule

TIME

- In the Last Hour
- Last 24 Hours**
- Yesterday
- This Week
- Last 30 Days

EVENT TYPE

- Command & Control**
- Cryptomining
- Malware
- Phishing
- Other Categories

Group Events by Type

RESPONSE

1 of 1 < >

SEARCH Security Activity **Advanced**

**All Security Activity (Last 24 Hours)**

Time	Activity Count
12:00 pm	0
5:00 pm	0
10:00 pm	15
3:00 am	15
8:00 am	10
10:00 pm	15

LAST 24 HOURS

PHISHING	<span style="color: red;">●</span> BLOCKED	Resolver ofelia.rediris.es BIND	+1	oct. 13, 2022 9:50 AM	▼
www.internetbadguys.com					
MALWARE	<span style="color: red;">●</span> BLOCKED	Resolver ofelia.rediris.es BIND		oct. 13, 2022 1:41 AM	▼
195-154-42-43.rev.poneyt...					



RedIRIS



# Aspecto del tenant

**Cisco Umbrella**

[VOLVER AL PRINCIPIO](#)

www.internetbadguys.com **Phishing Lista de bloqueo**

Talos Google VirusTotal

Amenaza	Tipo de amenaza	Aplicación relacionada
-	-	internetbadguys

Categorías de contenido	Categorías de seguridad	Categoría de la aplicación	Proveedor
Computer Security	Phishing	Website	internetbadguys

[Categorización de disputa](#)

**Puntuación de riesgo**

**18** **Bajo riesgo**

El dominio se clasifica como de bajo riesgo. No encontramos amenazas maliciosas ni características de seguridad sospechosas. [INDICADORES DE SEGURIDAD](#)

**Creado el** 02/28/2006 (16 años) **Pais/Región del solicitante de registro** US

IP reciente	Pais/Región de IP	Prefijo	ASN	Descripción del propietario de la red
146.112.255.155	US	146.112.255.0/24	AS36692	OPENDNS, US 86400

**SECURE X** Home Enrich... ? +



Red IRIS



# ¡Muchas gracias!

## Contactos:

- [jcarlos.rodriguez@rediris.es](mailto:jcarlos.rodriguez@rediris.es)
- [dnsfirewall@rediris.es](mailto:dnsfirewall@rediris.es)

## Mas info:

- <https://www.rediris.es/dnsfirewall/>



Red IRIS

