Servicio DNS FIREWALL De

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

Que es un DNS Firewall: Arquitecturas

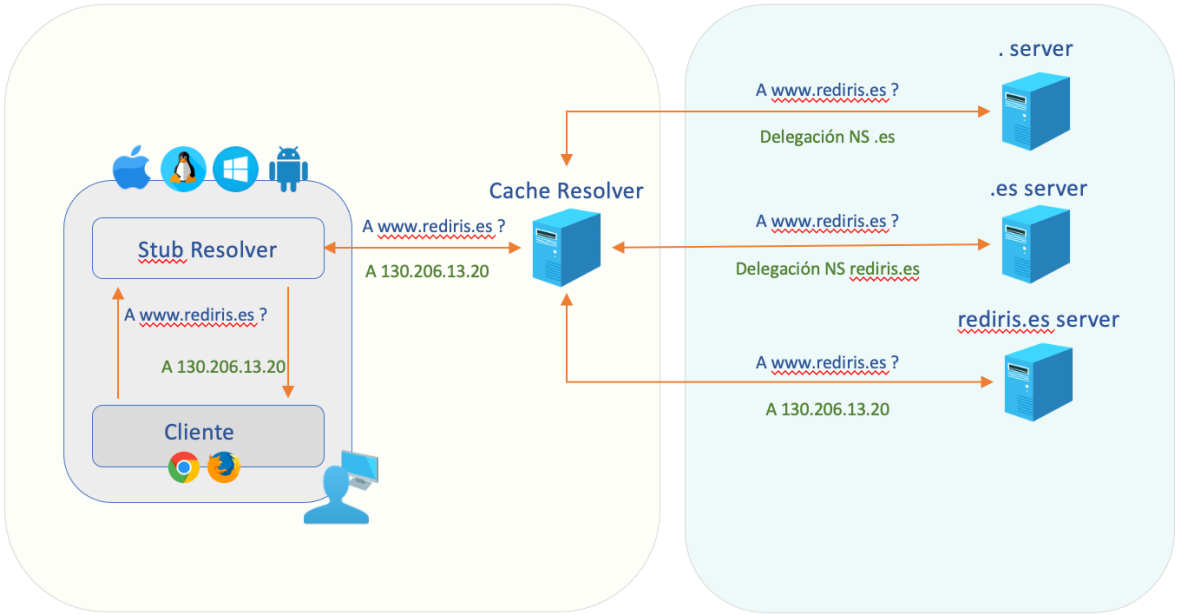
Zonas RPZ integradas en los resolvers de las organizaciones:

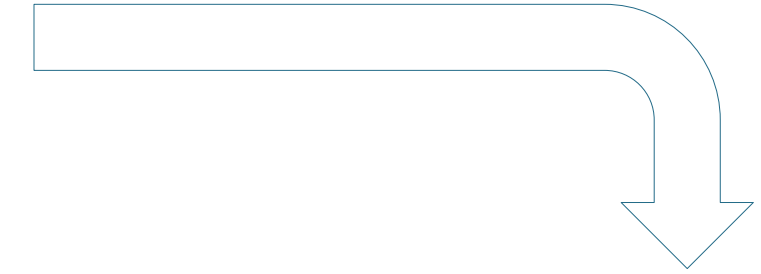
- Contienen listas de sitios maliciosos y políticas
- Zonas RPZ comerciales de proveedores de seguridad (Free-€-€€)
- Reactivas (listas actualizadas a posteriori)

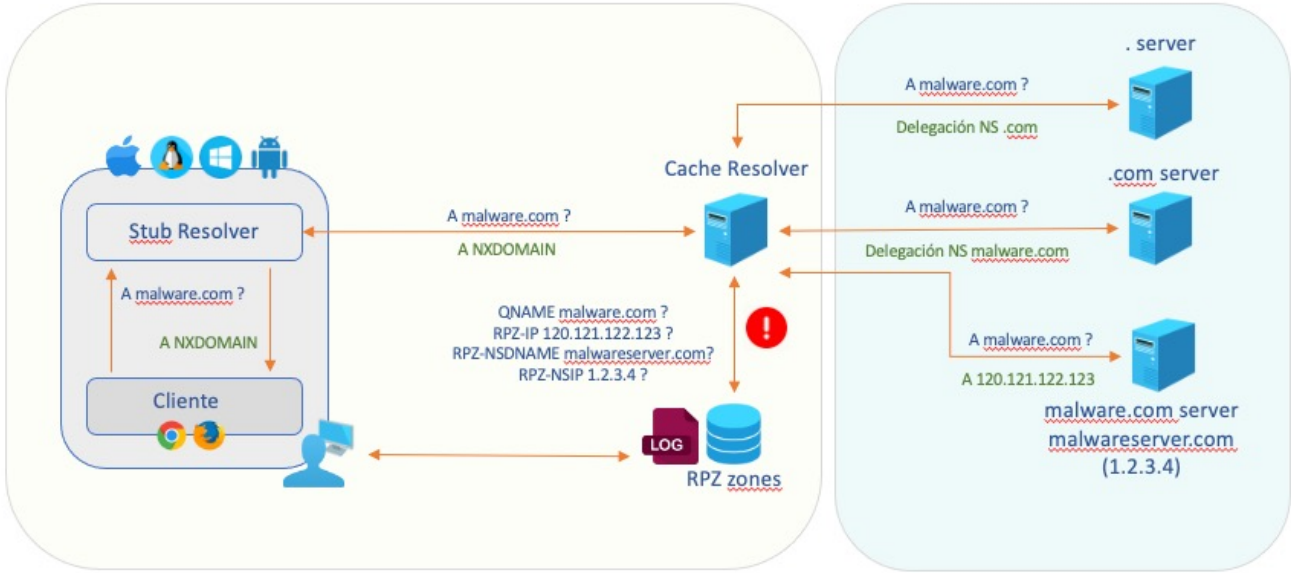
Servicios DNS Firewall cloud especializados

- 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)

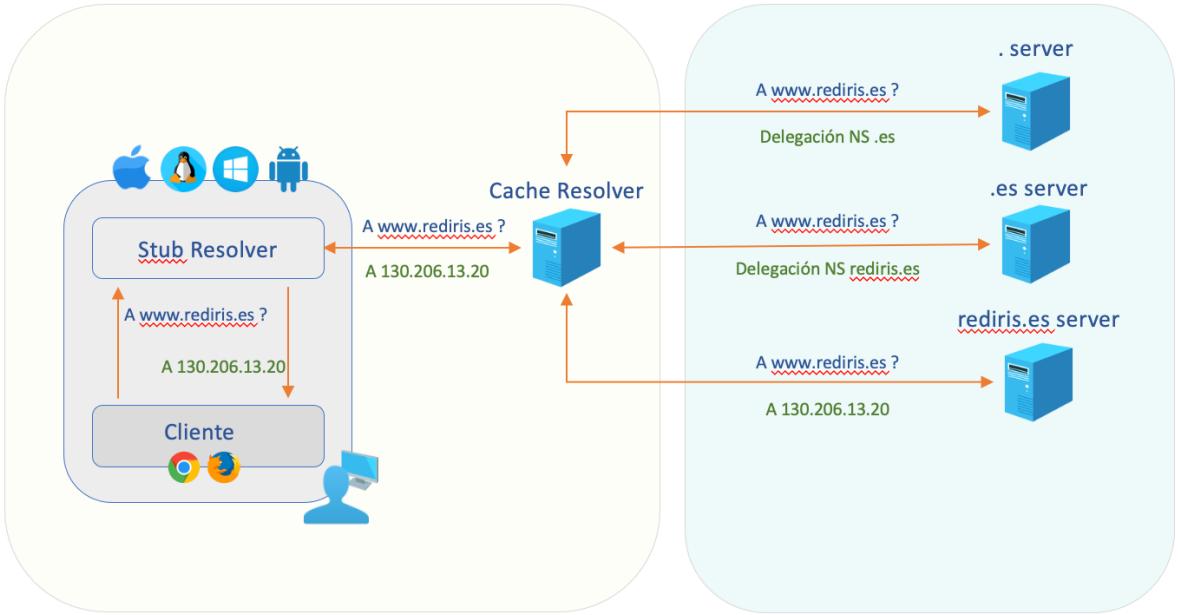
DNS Firewall: Protección RPZ

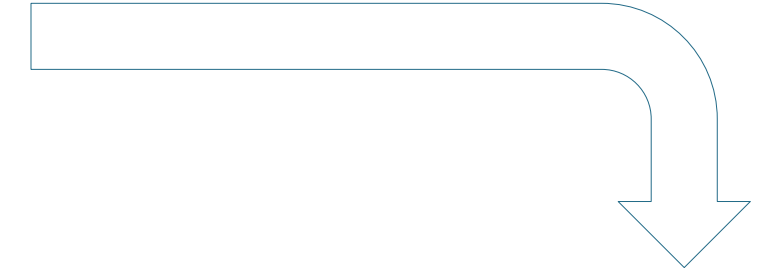


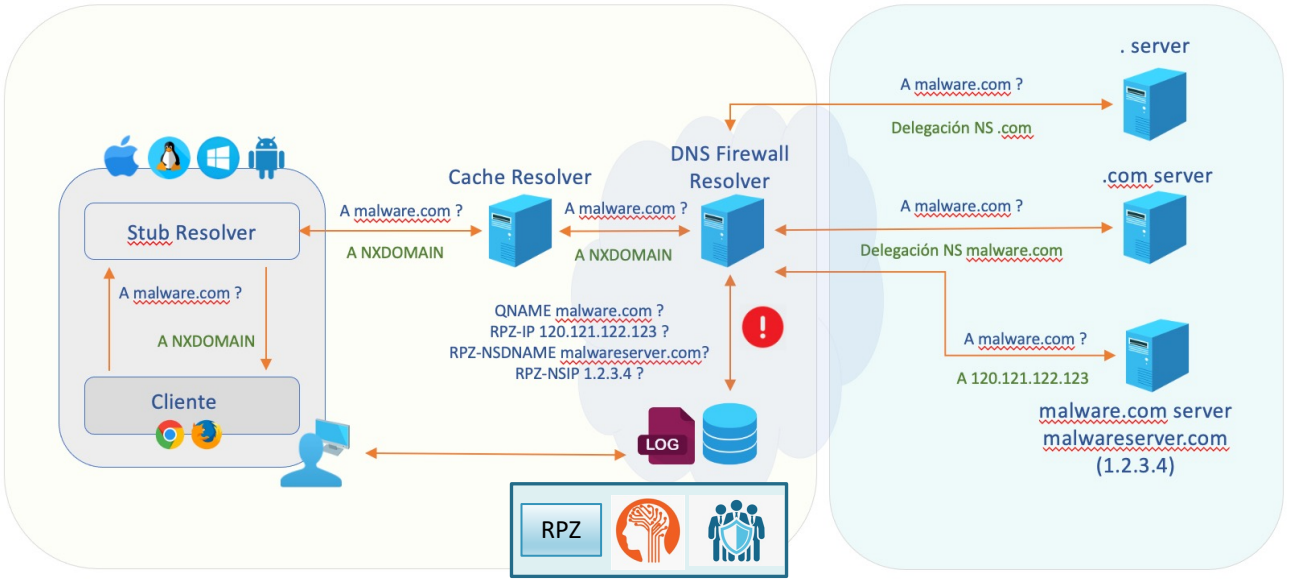




DNS Firewall: Protección Servicio Cloud







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

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

- Atención de incidencias 24x7 para incidencias:
  - Contacto vía correo electrónico a 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.

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.

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

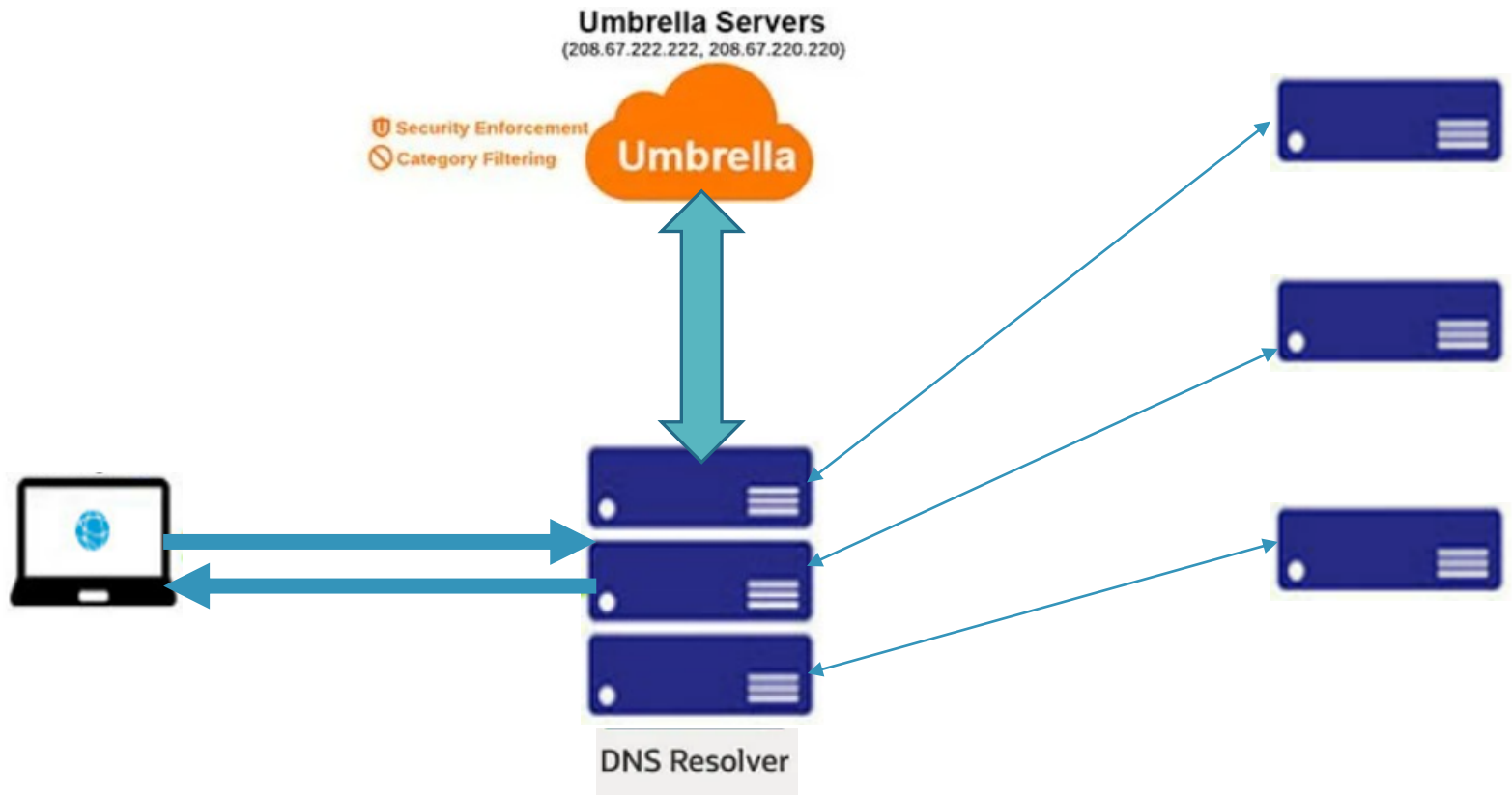
Hay varios escenarios para integrar CISCO UMBRELLA en nuestra red:

- 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

Escenario 1: Hacer forwarding de nuestro resolver a Umbrella



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

Escenario 1: Cómo hacer el forwarding:

DNS BIND:

- *# Configuracion 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:*

  # Configuracion 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

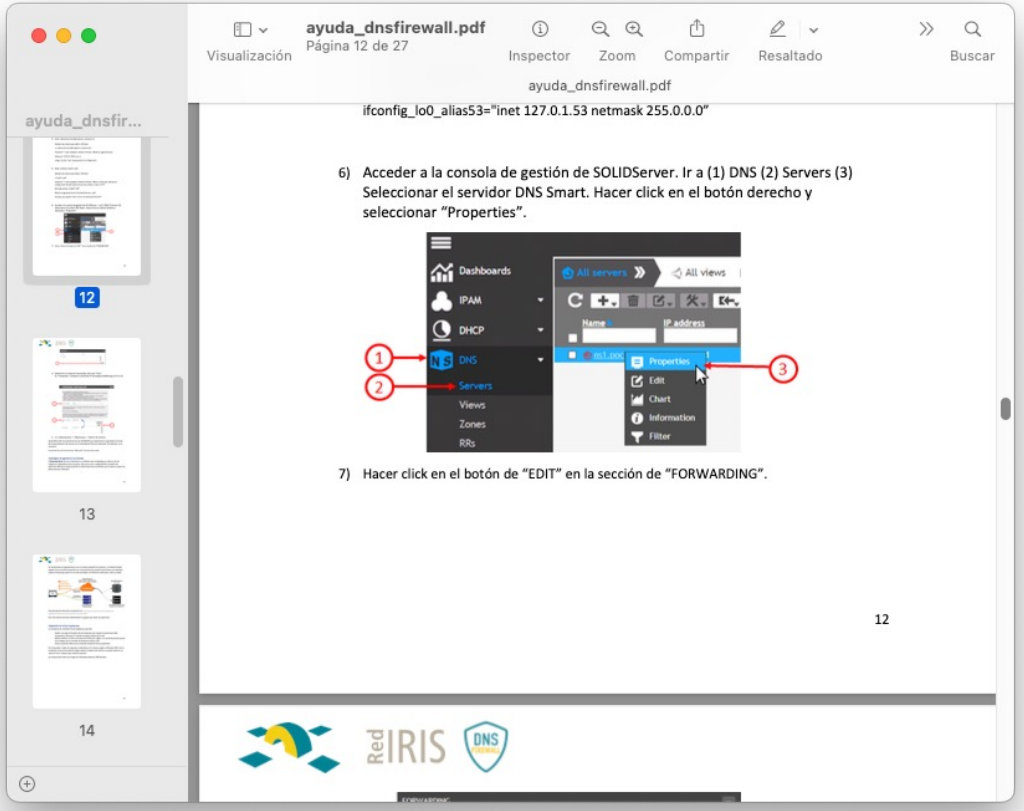
  (2) Reiniciar el servidor para aplicar la configuración.

  $ systemctl restart pdns-recursor

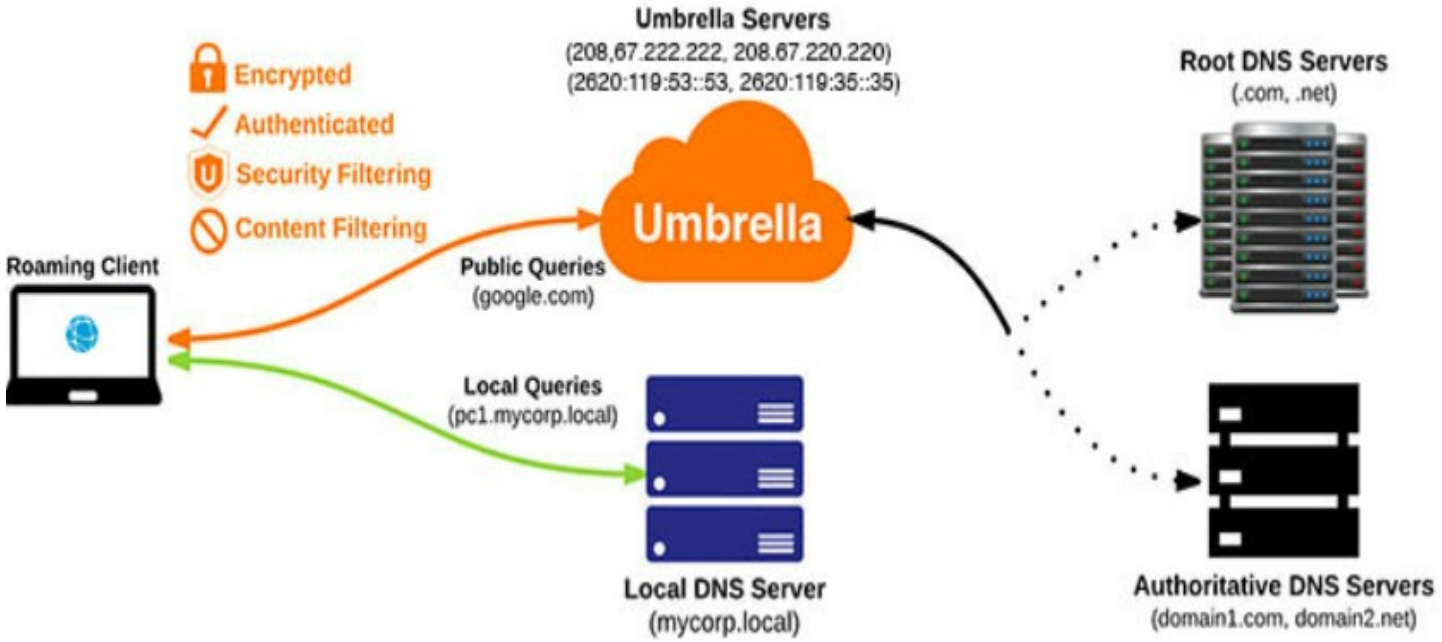
Escenario 1: Guía de primeros pasos y configuración

Infoblox, Efficientip, Microsoft…

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

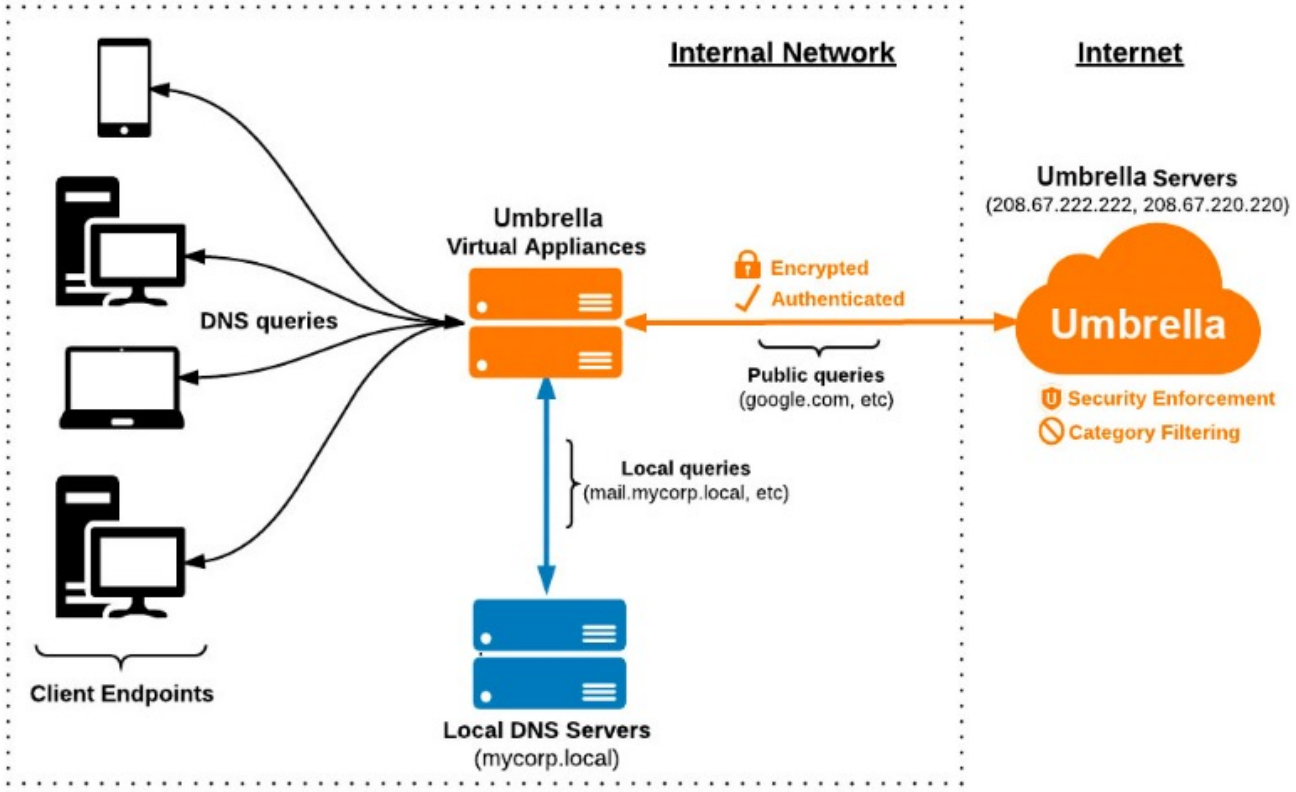


Escenario 2: Desplegar Agentes



- 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)*
- Con este sistema tenemos identificados lo equipos que hacen las peticiones.

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

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.

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.

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. (báisco + new and Dynamic domains, potentially harmful)

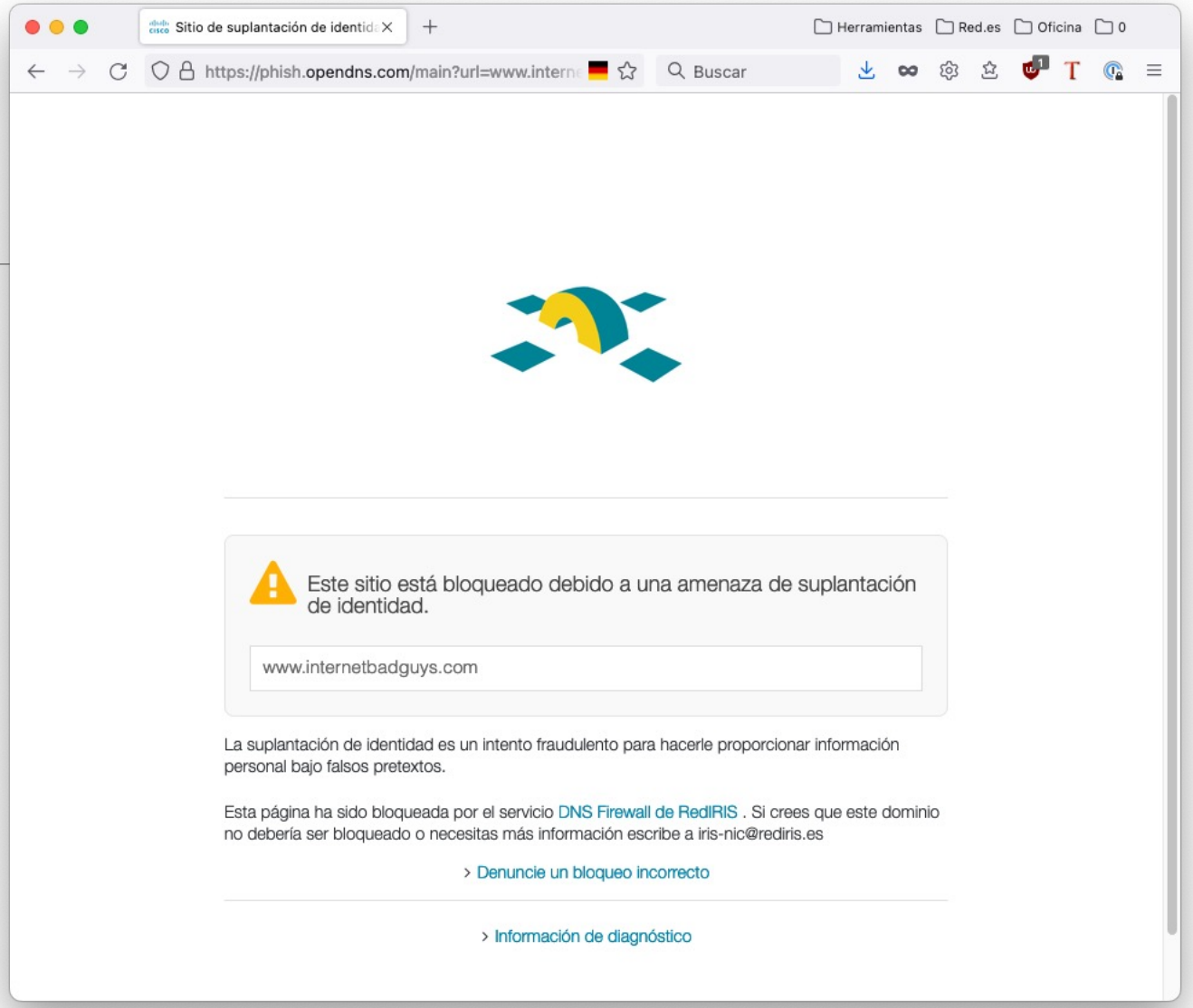
Las redes están configuradas. Se pueden hacer subnetting.

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

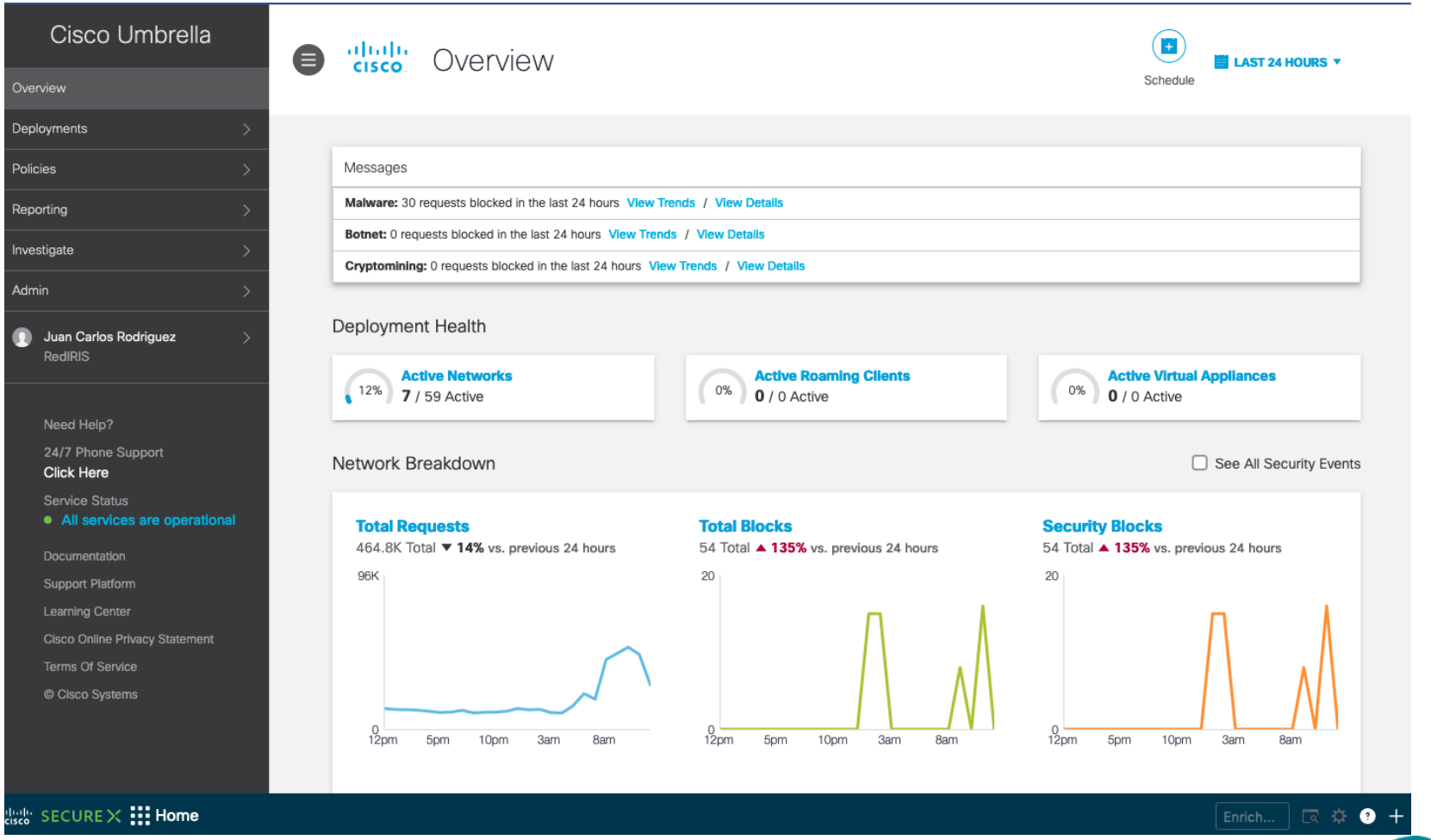
Configuración Inicial del tenant

Varios comportamientos:

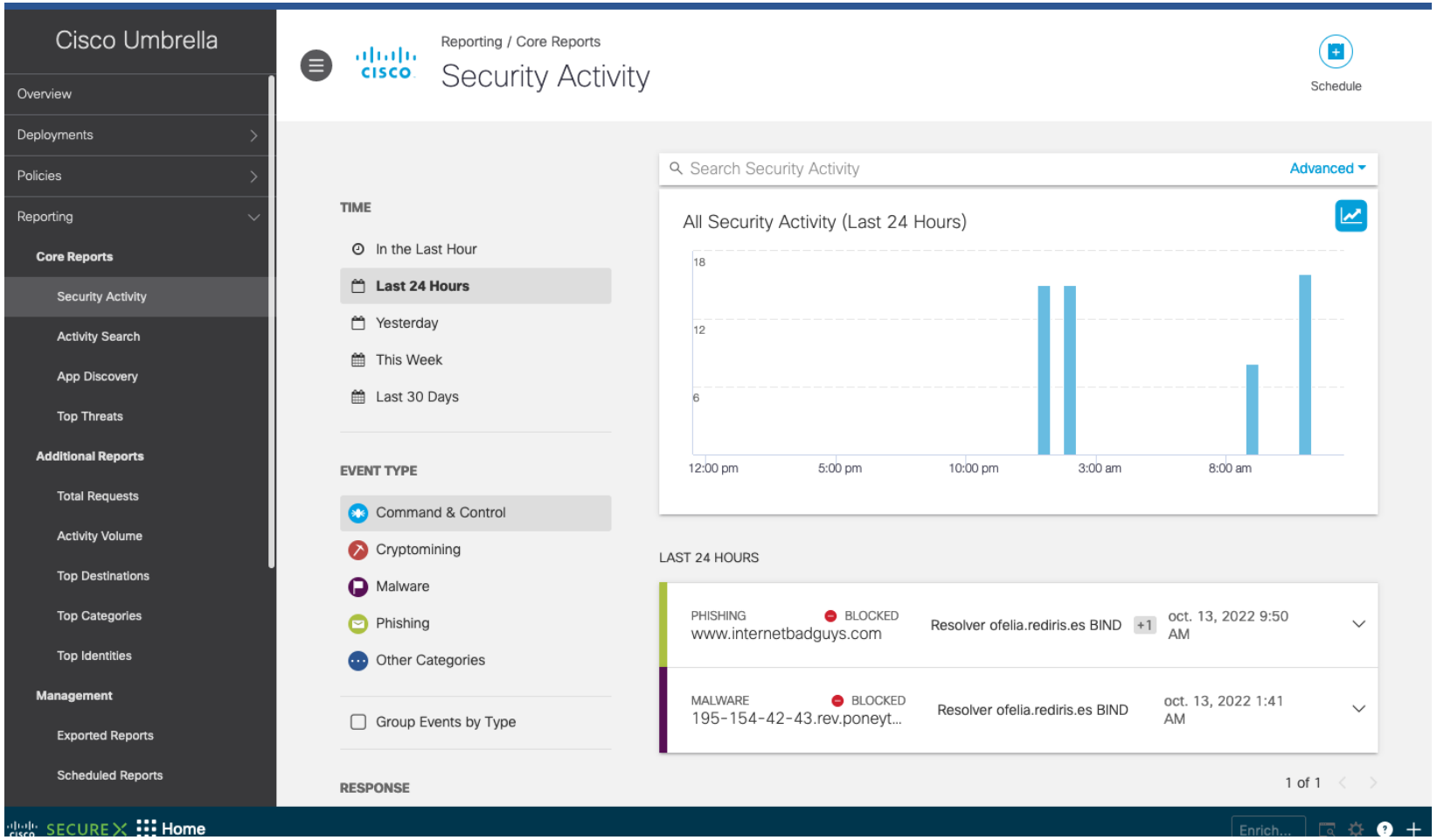
- Redirección web
  - pagina personalizable
  - a URL externa
- No responder
- Respuesta no existe el dominio…



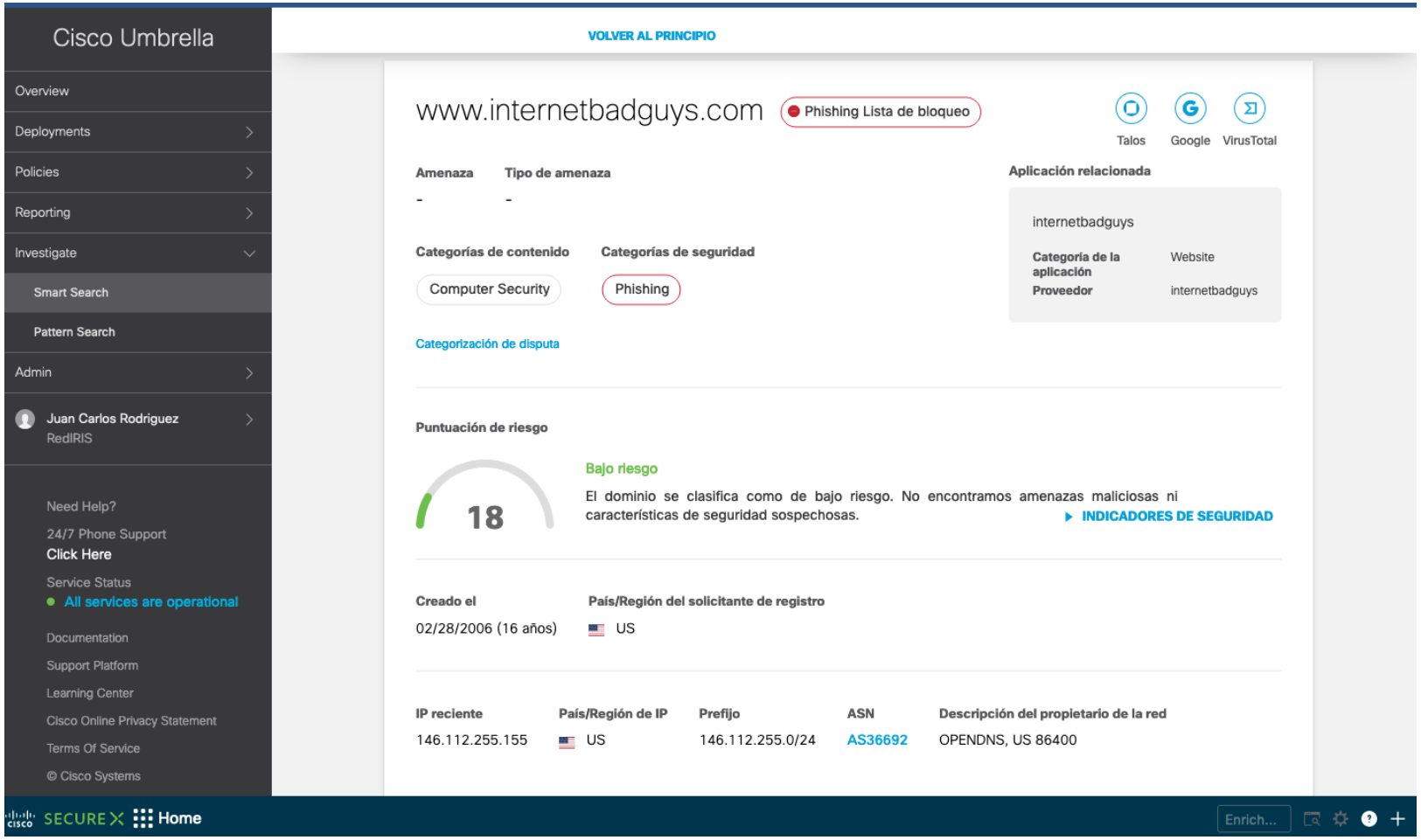
Aspecto del tenant



Aspecto del tenant



Aspecto del tenant



¡Muchas gracias!

Contactos:

- jcarlos.rodriguez@rediris.es
- dnsfirewall@rediris.es

Mas info:

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