Servicio DNS Firewall de RedIRIS: *Guía de primeros pasos y configuración inicial*

Versión 1.10 – 13/04/2023

Que es un DNS Firewall

El protocolo DNS se encarga de facilitar el uso de los recursos informáticos al traducir las direcciones IP a nombres, llamados dominios. Además de ser más fácil de recordar, el nombre es más fiable. La mayoría de las comunicaciones legítimas y no legítimas, tanto de usuarios, como de servidores y elementos del Internet de las Cosas comienzan con una consulta DNS.

Las mayores fortalezas de este protocolo es que es muy abierto, descentralizado y fiable, pero a menudo los ataques de malware, phising y botnets hacen uso de estas características en contra de los usuarios.

Un DNS firewall es una herramienta de seguridad, adicional y complementaria a los firewalls tradicionales y otras herramientas de inspección de tráfico, enfocado únicamente al tráfico DNS y que se encarga de redirigir o bloquear el acceso de los usuarios finales a sitios maliciosos.

RedIRIS pone a disposición de sus instituciones un servicio de DNS Firewall basado en la plataforma Cisco Umbrella.

Servicio DNS Firewall de RedIRIS

Plataforma del servicio

El servicio DNS Firewall de RedIRIS usa la plataforma Cisco Umbrella que tiene las siguientes características:

- 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 resolvers del servicio.

Cisco Umbrella es un servicio en la nube que proporciona defensa contra las amenazas en Internet sin importar dónde se encuentren los usuarios. Permite tener visibilidad completa de la actividad DNS en todas las ubicaciones y dispositivos, y detiene las amenazas antes de que lleguen a la red de la organización o a sus usuarios, bloqueando de forma proactiva las solicitudes a destinos maliciosos antes de que se establezca la conexión, sin añadir latencia adicional.

La red global Umbrella resuelve a diario miles de millones de solitudes alrededor del mundo. Estos datos se analizan para identificar patrones y descubrir la infraestructura de los atacantes usando modelos estadísticos y machine learning sobre ellos. Esta información también es analizada constantemente por los investigadores de seguridad de Umbrella y complementada con la inteligencia de Cisco Talos. Mediante esta combinación de inteligencia humana y machine learning se identifican sitios maliciosos (tanto dominios, direcciones IP o URL) en Internet.

Umbrella se integra también con otras soluciones de seguridad. Puede enviar los datos de registro de la actividad a un SIEM y/o a sistemas de gestión de syslog, y usando la API permite modificar las listas de bloqueo aplicadas.

RedIRIS pone a disposición de su comunidad el servicio Cisco Umbrella mediante la licencia DNS Security for Education, centrada en el bloqueo del tráfico DNS, aunque existen otros modos de licencia no cubiertos por este servicio.

Al ser un servicio multitenant o multihilo, cada institución tendrá la capacidad de gestionar una instancia personalizada, con sus propias políticas de seguridad e información de bloqueo.

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.

Solicitud de alta en el servicio

Para realizar el alta en el servicio es necesario realizar una petición al buzón dnsfirewall@rediris.es adjuntando el siguiente formulario.

Durante el proceso de alta, se pedirá que el PER de la institución firme las condiciones de uso disponibles para el servicio.

Adicionalmente, las organizaciones que previamente hayan trabajado con Cisco Umbrella o haya tenido un TRIAL o un DEMO de la herramienta, tienen que abrir un caso con soporte de Umbrella indicando que necesitan que se desactiven las redes que tienen dadas de alta en Umbrella porque van a poner en producción otro tenant.

Para abrir un caso con Cisco Umbrella hay que mandar un correo a: **umbrella-support@cisco.com**.

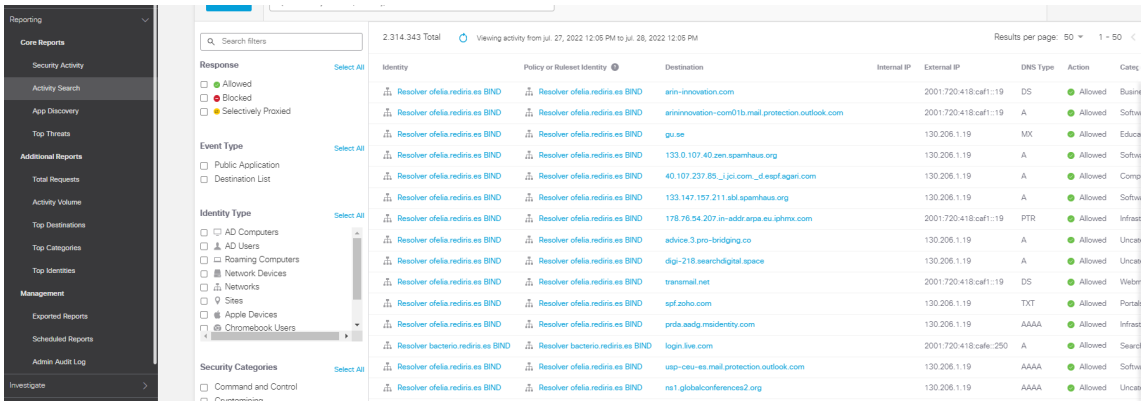
Configuración inicial del servicio

RedIRIS ha generado tres tipos de políticas de seguridad centralizadas que pueden ser utilizadas directamente sin requerir modificaciones:

- ***Modo transparente***: no aplica bloqueos, solo inspecciona el tráfico y pone a disposición del administrador todo el histórico de consultas y amenazas detectadas.
- ***Modo de seguridad básico***: aplica los siguientes bloqueos:
    - **Malware**: *"Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more."*
    - **Command and Control Callbacks**: *"Prevent compromised devices from communicating with attackers' infrastructure."*
    - **Phishing Attack**: *"Fraudulent websites that aim to trick users into handing over personal or financial information."*
    - **DNS Tunneling VPN**: *"VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer."*
    - **Cryptomining**: *"Cryptomining allows organizations to control cryptominer access to mining pools and web miners."*
- ***Modo de seguridad alto***: aplica los bloqueos del modo de seguridad básico y añade:
    - **Newly Seen Domains**: *"Domains that have become active very recently. These are often used in new attacks."*
    - **Dynamic DNS**: *"Block sites that are hosting dynamic DNS content."*

- **Potentially Harmful Domains**: *"Domains that exhibit suspicious behavior and may be part of an attack."*

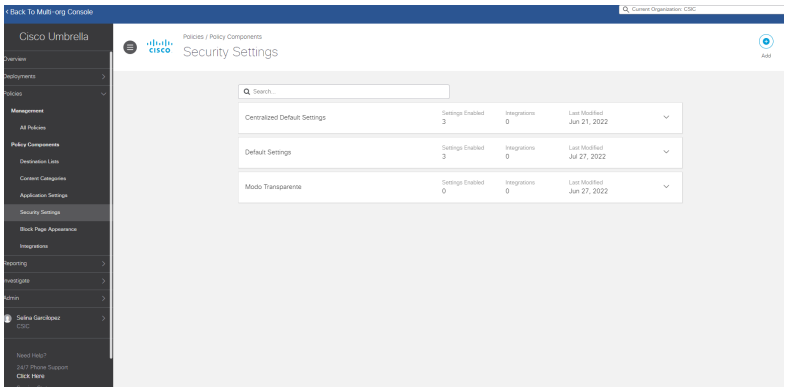
La configuración inicial del tenant se entrega en **Modo Transparente.** No se realizan bloqueos, aunque todas las peticiones DNS se realizan a través de Umbrella. Se puede ver toda la actividad en los gráficos y los reportes que genera la herramienta, siempre con el tráfico ***Allowed***:



Una vez puesto en producción el tenant, se puede solicitar cambiar a un nivel de seguridad básico o alto. Los administradores también podrán crear y gestionar sus propias políticas según los criterios de seguridad y las necesidades de la propia organización.

Como pasos previos a la puesta en producción es importante:

- En ***Deployments>Core Identities>Networks*** comprobar que el direccionamiento es el correcto.
- En ***Admins> Accounts*** se despliega el usuario y hay que:
  - Activar el 2FA, en el propio usuario, ya que se lo tiene que activar uno a si mismo cuando es un usuario administrador.
  - Seleccionar la zona horaria: ***(Timezone). UTC+02:00 Europa/Madrid***.
- Comprobar que se está aplicando el ***Modo Transparente*** en ***Policies>Security Settings***



Despliegue de la herramienta.

Hay distintos escenarios o arquitecturas posibles para el despliegue de la herramienta:

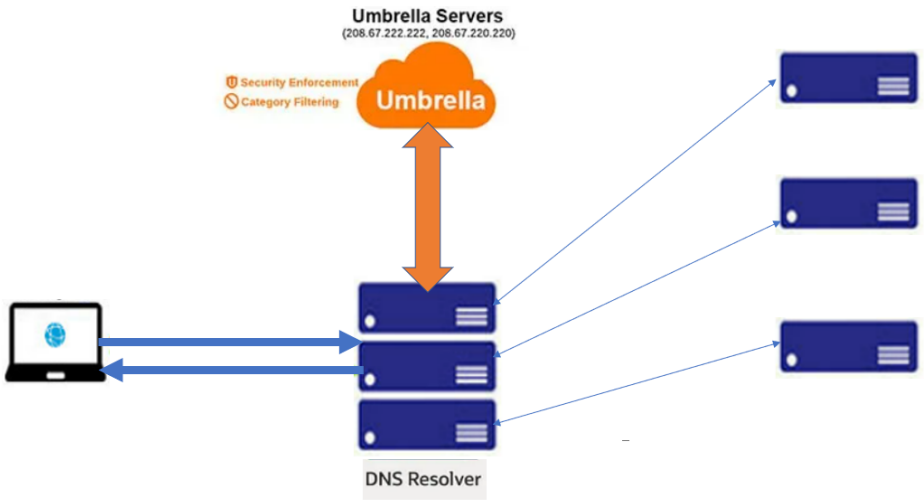
- Redirigir el DNS Resolver de la institución hacia Cisco Umbrella.
- Instalación de Virtual Appliances.
- Despliegue de agentes en los dispositivos de los usuarios. Compatible con las dos anteriores.

Configurar el DNS Resolver hacia Cisco Umbrella.

La integración más sencilla consiste en hacer *forwarding* en el DNS Resolver de la organización y redirigir todas las peticiones DNS externas a Cisco Umbrella.

El direccionamiento de Cisco Umbrella es:

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



De esta forma las peticiones son resueltas por Umbrella, que aplica la política de seguridad configurada, resolviendo o bloqueando la consulta y dejando el resultado en el log.

Es el escenario inicial recomendado, puesto que requiere poca configuración o modificación de la arquitectura DNS actual de la institución y permite usar la potencia de detección y bloqueado de Umbrella, pero tiene la desventaja de que no identifica la máquina original que realizó la consulta, puesto que a Cisco Umbrella le llega la petición con la dirección IP del resolver.

Configuración del *forwarding* según el tipo de Resolver:

BIND

Ejmplo de configuración para RHEL7, BIND 9.11 ejecutándose en entorno chroot:

(1) Añadir las siguientes sentencias en los fichero de configuración named.conf:

```
# Configuracion para DNS Firewall (servidores de Umbrella)
# Forwardinng 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;
```

(2) Comprobar la sintáxis y reiniciar el servidor (preferentemente)

```
$ named-checkconf
$ systemctl restart named-chroot (si el entorno es chroot)
$ systemctl restart named (si el entorno NO es chroot)
```

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
```

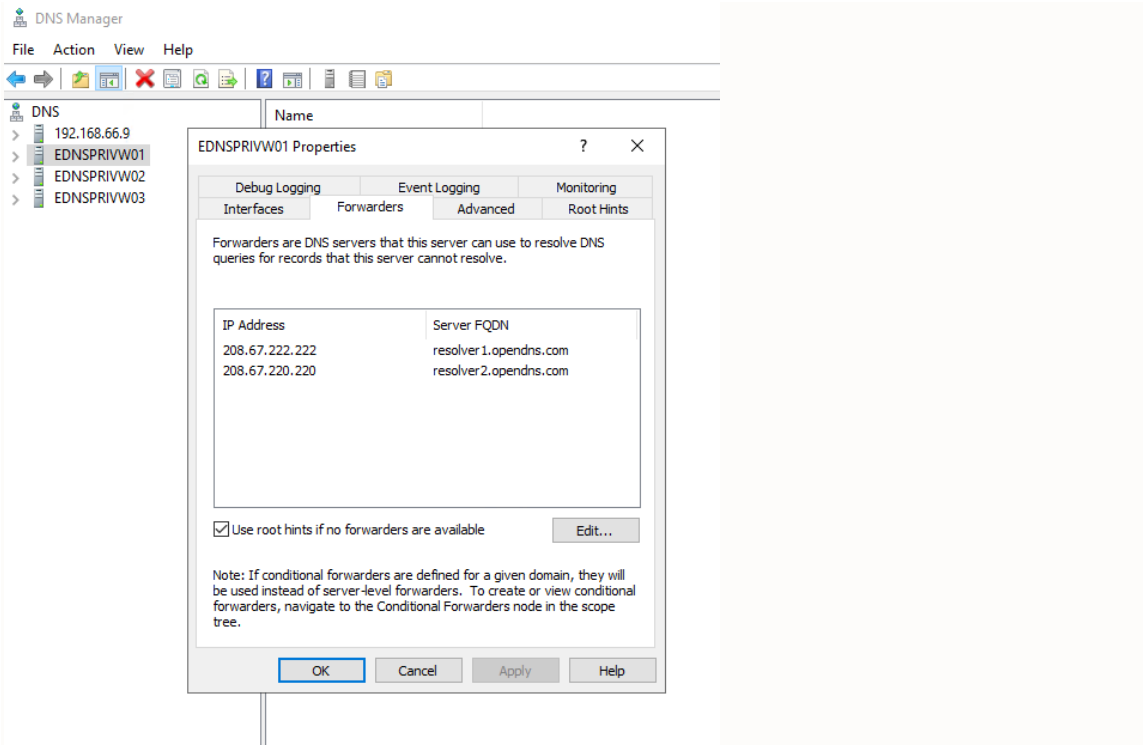
(2) Reiniciar el servidor para aplicar la configuración.

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

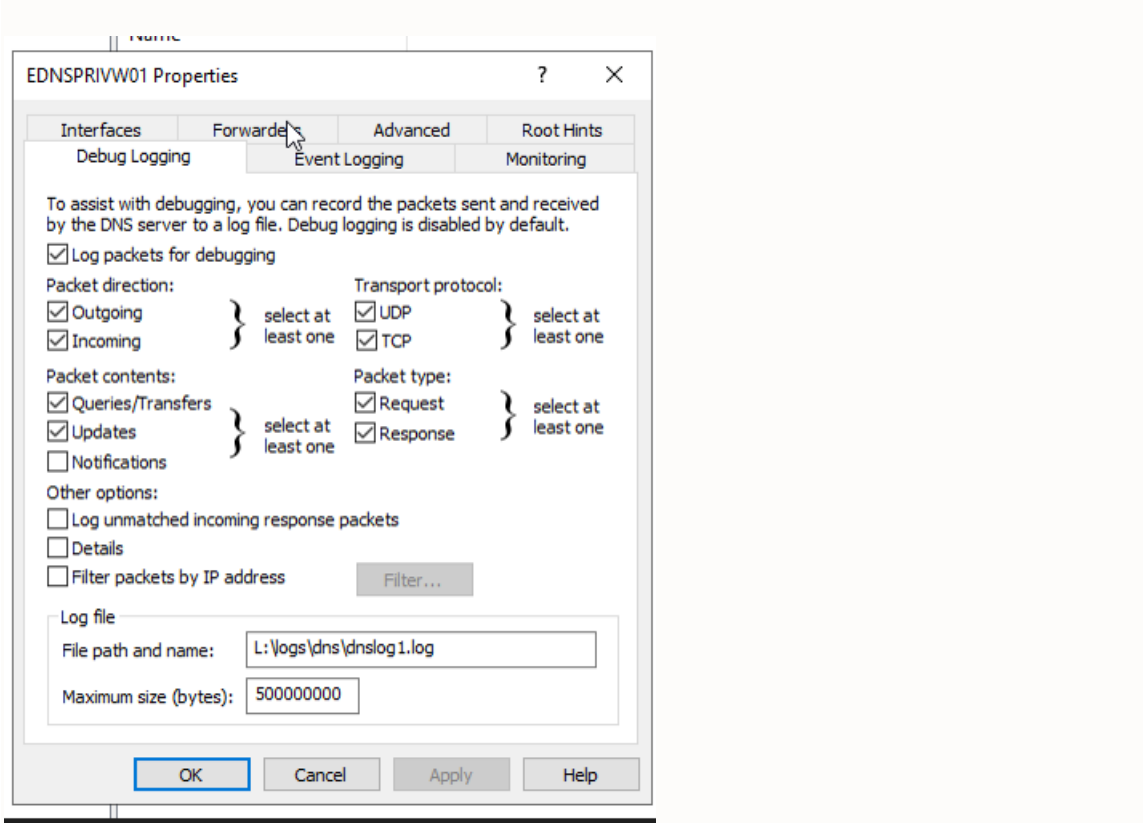
Microsoft

Dentro del servidor, en la pestaña "forwarders", se añaden las IP's de Umbrella.

Se puede dejar activa la opción "use root hints if no forwareders are available" por si Cisco Umbrella tuviera algún problema y no respondiera, que lo haga el resolver:



Se activa el Debug Logging para tener la trazabilidad de quien hace la petición.



Para activar el rotado del log se hace mediante powershell como administrador

```
Set-DnsServerDiagnostics -EnableLogFileRollover $true
```

Con esto queda configurado el servicio.

Infoblox

Directamente extraído de la documentación del fabricante:

"Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.

Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box ->Edit icon.

DNS View: From the Data Management tab, select the DNS tab -> Zones tab -> dns_view check box -> Edit icon.

Note that if there is only one DNS view— for example, the predefined default view—you can just click the Edit icon beside it

To override an inherited property, click Override next to it and complete the appropriate fields.

- *Click the Forwarders tab.*
- *Click the Add icon*
- *Enter an IP address in the text field. The field supports entry for both IPv4 and IPv6 values.*

To remove a forwarder, select the IP address from the Forwarders list, and then click the Delete icon.

To move a forwarder up or down on the list, select it and click the Up or Down arrow.

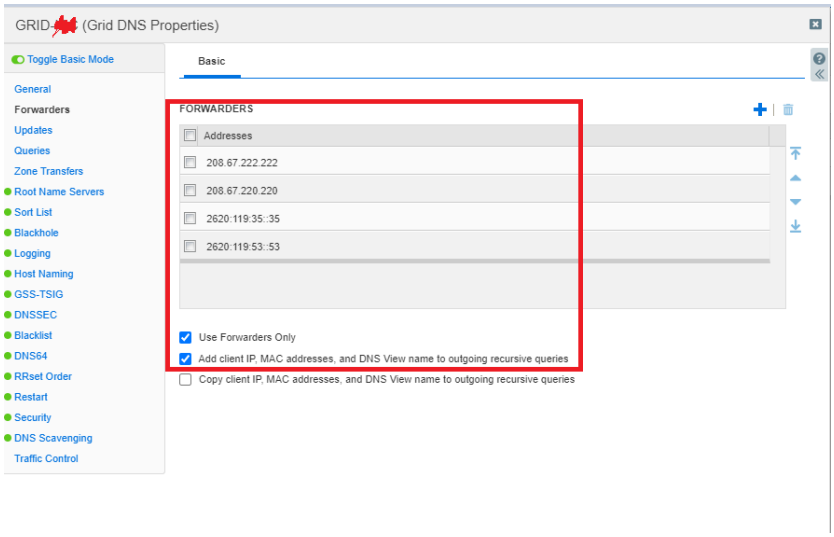
- *To use only forwarders on your network (and not root servers), select the Use Forwarders Only check box.*
- *Save the configuration and click Restart if it appears at the top of the screen"*

Guía rápida de configuración de Umbrella con Infoblox:

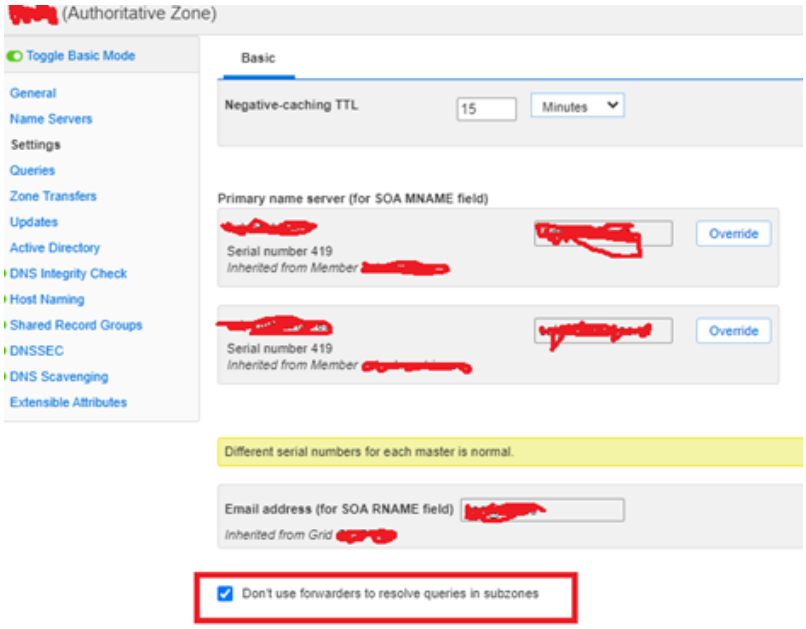
Las opciones necesarias para realizar la configuración en el sistema DNS del fabricante Infoblox y poder comenzar a hacer uso del filtrado DNS de Cisco Umbrella ofrecido por RedIRIS son las siguientes:

1) *A nivel de GRID DNS debemos colocar la siguiente configuración en la pestaña "Forwarders" definiendo todas las IPs (IPv4 e IPv6 si fuese el caso) de los servidores de Umbrella y marcando la opción "Use Forwarders Only".*

   Es importante que marquemos también la opción "Add IP Client, MAC Addresses…" ya que con ello podremos ver el IP del cliente que ha originado la consulta y por tanto una visibilidad asequible; situación que siempre podremos mejorar con el despliegue de las máquinas virtuales de Umbrella si fuese es necesario.



2) *Si además tuviésemos dominios DNS delegados (principalmente aquellos que no son visibles desde Internet) y no deberíamos reenviar las consultas sobre ellos a la nube de Umbrella por lo que debemos activar la siguiente opción "Don´t use forwarders to resolve queries in subzones" dentro de la zona DNS padre de la afectada. Si no realizaremos esta excepción, todas las consultas sobre este tipo de subdominios no obtendrían respuesta correcta desde Umbrella (la respuesta sería NXDOMAIN, dominio desconocido), por lo que provocaría fallos de conectividad a nuestros clientes.*



EfficientIP

Documentación en el enlace https://learn-umbrella.cisco.com/feature-briefs/efficient-ip-feature-brief

Añadir información de cliente:

- https://umbrella.cisco.com/blog/now-available-efficientip-and-cisco-umbrella-integration (versiones antiguas)
- Versiones más recientes:

```
[...]
     192.168.99.0/32 is subnetted, 1 subnets
i L1     192.168.99.8 [115/20] via 192.168.1.50, 00:00:33, FastEthernet0/0
[...]

router>  show clns neighbors
System Id      Interface   SNPA            State  Holdtime  Type Protocol
dns-anycast-1  Fa0/0       000c.29ef.d8bb  Up     28        L1   IS-IS
```

To display the IS-IS neighbors status on SOLIDserver

1. Connect to SOLIDserver via a shell session.
2. Run the following command to connect to the zebra service:

```
% vtysh
Hello, this is Quagga (version 1.1.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
dns-anycast-1#
```

3. 3. Run the following command to display info on IS-IS neighbor:

```
dns-anycast-1# show isis neighbor
Area ISIS_0:
  System Id           Interface   L  State        Holdtime SNPA
  router                          em3         1  Up           8            ca01.025d.0000

dns-anycast-1# show isis hostname
Level  System ID      Dynamic Hostname
1      1720.1600.1001 router
*      1720.1600.2002 dns-anycast-1
```

Integrating Cisco Umbrella

SOLIDserver embeds a DNSCrypt proxy which allows you to forward all the DNS queries it receives to the Cisco Umbrella Cloud[2].

DNSCrypt is a protocol that authenticates communications between a DNS client and a DNS resolver. It prevents DNS spoofing. It uses cryptographic signatures to verify that responses originate from Cisco Umbrella and haven't been tampered with.

To successfully configure SOLIDserver for Cisco Umbrella:

1. Via Cisco Umbrella web interface, create a network device and retrieve its API key and secret strings.
2. Via SOLIDserver GUI, configure the IP address dedicated to Umbrella as the *only* forwarder for your local DNS appliance.
3. Via SOLIDserver CLI, configure and launch the proxy DNSCrypt.

Note that:

- The DNSCrypt protocol uses the port 443, in TCP and UDP, which is usually reserved to HTTPS. It is possible that some equipments, such as firewalls, IDP or IPS detect a wrongful use of the port. Make sure these equipments are configured to allow this traffic.
- You cannot integrate Cisco Umbrella on Hybrid servers. For more details on Hybrid servers, refer to the chapter Hybrid DNS Service.
- Once you integrated Cisco Umbrella, you can complete the CLI configuration and forward the client IP address. For more details, refer to the section Forwarding the Client IP Address.

To configure the appliance for Cisco Umbrella

Only users of the group *admin* can perform this operation.

1. **Retrieve your Cisco Umbrella parameters**
   a. Connect to your Cisco Umbrella web interface using your credentials.
   b. In the left panel, click on **Admin > API Keys**. The page refreshes.
   c. Tick the box **Umbrella Network Devices**.
   d. Click on CREATE. The page refreshes and displays **Your Key** and **Your Secret** strings. Copy these values and keep them at hand as they disappear after you leave this page, you need them later on during the configuration.
   e. Tick the confirmation box and click on CLOSE.
2. **Configure the DNS forwarder from the GUI**
   a. In the sidebar, go to **DNS > Servers**. The page **All servers** opens.
   b. At the end of the line of the server or smart architecture you intend to connect to Cisco Umbrella Cloud, click on . The properties page opens.
   c. Open the panel **Forwarding** using .
   d. Click on EDIT. The wizard **Forwarding configuration** opens.
   e. In the field **Add a forwarder**, type *127.0.1.53* which is the IP address dedicated to the proxy DNSCrypt.
   f. Click on ADD to move it to the list **Forwarders**.
   g. In the field **Forward mode**, select *Only*.
   h. Click on OK to complete the operation. The report opens and closes. The properties page refreshes and displayed the new settings.
   i. Repeat step *c* to *i* for each server or smart architecture on which you plan to deploy DNSCrypt.
3. **Configure and launch the proxy DNSCrypt via CLI**
   a. Open a shell session and connect to your appliance as the default *admin* user, the default password is *admin*, or using the credentials of a user with *sudo* permissions.
   b. Get *root* access using the following command:

```
sudo -s
```

   c. Retrieve your DNSCrypt parameters using the script *umbrella_setup*. You must specify the API key and API secret you copied earlier and the name of the device of your choice, as defined in your *Network Devices* list, as follows:

```
/usr/local/nessy2/script/umbrella_setup <Your-Cisco-Umbrella-API-Key>
<Your-Cisco-Umbrella-API-Secret> <Your-Network-Devices-Cisco-Umbrella-Device-Name>
```

   The result should look as follows:

```
server 127.0.1.53 {
    edns-opendns yes;
    edns-opendns-orgid <your-Cisco-Umbrella-Organization-ID>;
    edns-opendns-deviceid "<your-Cisco-Umbrella-Device-ID>";
};
```

   d. Copy the lines returned.
   e. Edit the DNS *global* include file.
      1. Open the `/data1/etc/namedb/global_include.conf`.
      2. Copy the lines of the DNSCrypt global parameters your retrieved.

3. Save your changes.

f. Edit the DNS *options* include file.
   1. Open the `/data1/etc/namedb/options_include.conf`.
   2. Add the following line to the file, to specify DNSCrypt options parameters:

```
listen-on { !127.0.1.0/24; any ; };
```

   3. Save your changes.

g. Edit the system configuration file.
   1. Open the file `/etc/rc.conf`.
   2. Edit it to enable the proxy DNSCrypt as follows:

```
dnscrypt_proxy_enable="YES"
```

   3. Add the following line to the file to specify the IP address dedicated to the proxy DNSCrypt:

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

   4. Save your changes.

h. Restart the network configuration using the command:

```
/etc/netstart
```

i. Start the service *dnscrypt-proxy* using the command:

```
/usr/local/etc/rc.d/dnscrypt-proxy start
```

j. Restart the service *ipmdns* using the command:

```
/usr/local/etc/rc.d/ipmdns.sh restart
```

Now, every DNS query trafficking through the appliance is directly forwarded to the Cisco Umbrella Cloud for resolution using your organization ID and device ID, and therefore, your Umbrella policies.

k. Repeat all the steps for each appliance you want to configure.

Forwarding the Client IP Address

Via CLI, you can configure EfficientIP DNS and BIND recursive servers to forward the IP address of the client that performed the original query.

If you have cascaded several resolvers, the IP address of a client is overwritten every time it is forwarded. Therefore, once the query gets to the resolver that actually performs the resolution, the source IP address it receives is no longer the one of the original client. Forwarding the original client IP address between resolvers allows to track it, no matter how many resolvers forwarded the original query.

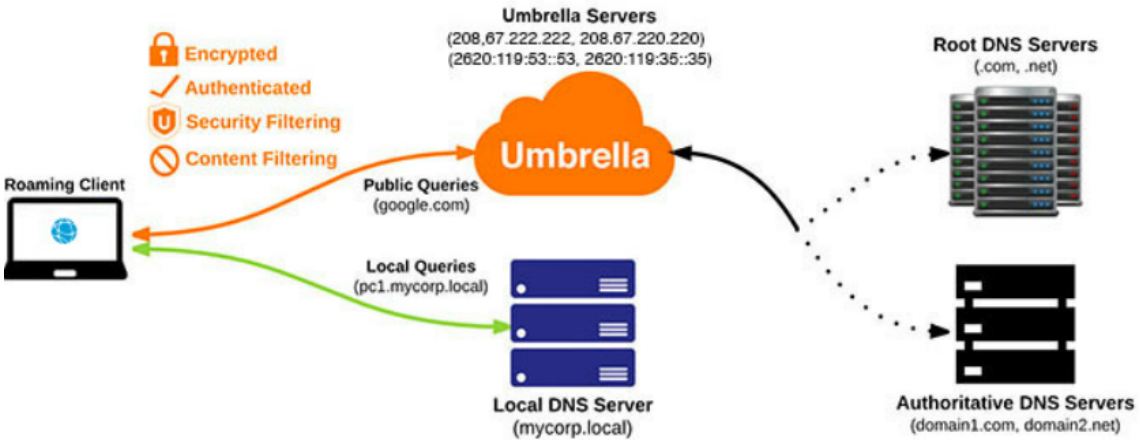
To enable forwarding of the client IP address, you must configure the statement `server` with the following options:

- *edns-opendns* set to *yes*.
- *edns-opendns-orgid* set with the administrative value of your choice, it must be composed of digits. If you did not integrate Cisco Umbrella you can specify any value, otherwise you must specify the relevant organization ID.

Despliegue de agentes en los clientes

El **Roaming Client** de Cisco Umbrella es un software que se despliega en cada una de las máquinas o dispositivos de los usuarios, bien una a uno o mediante GPO. Encamina las peticiones DNS de la máquina donde se instala hacia Cisco Umbrella y por lo tanto no pasan las peticiones por el Resolver.

Se recomiendo en organizaciones con un número pequeño de usuarios, o en determinados equipos de una institución grande con características de conexión particulares, por ejemplo, euipos en Roaming cuando no se está conectado a la VPN de la institución o ésta no existe.



Documentación oficial de la instalación en https://docs.umbrella.com/umbrella-user-guide/docs/download-and-install-the-roaming-client

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

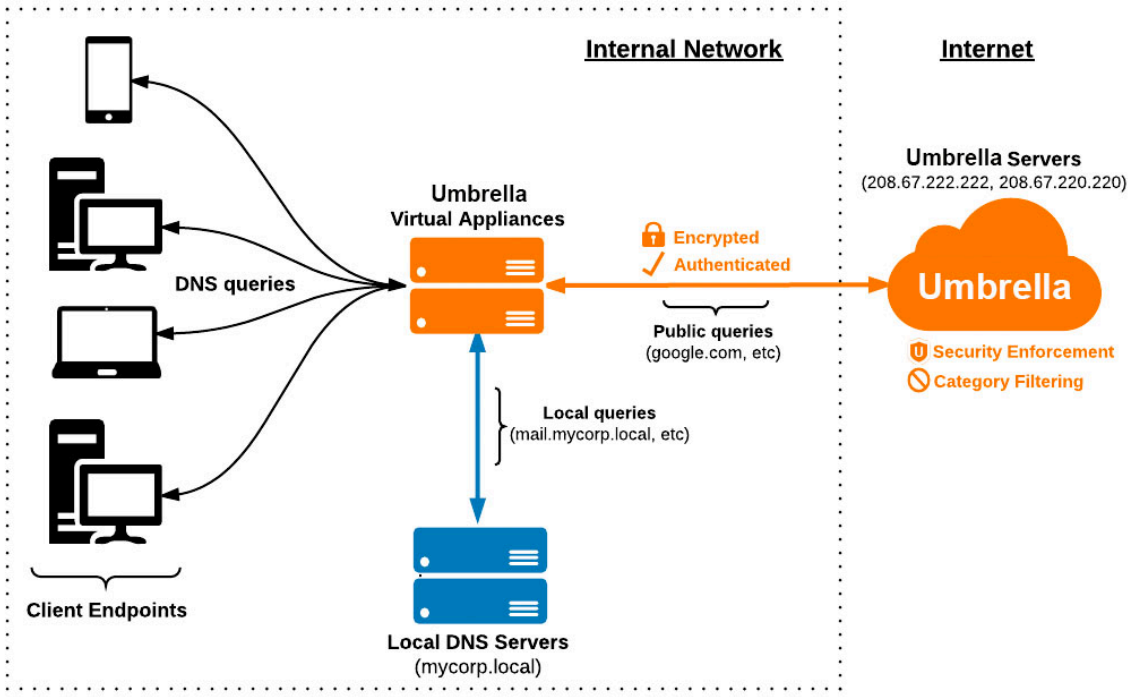
Instalación de Virtual Appliances.

La instalación de Umbrella Virtual Appliances permite:

- Añadir a los logs información de las máquinas que realizan las peticiones DNS, incluyendo la dirección IP real de la máquina dentro de la red.
- Aplicar políticas no sólo en función de la dirección origen, si no de atributos del usuario (si se integra con un servidor de directorio activo o AD)
- Enviar la petición DNS a Cisco Umbrella cifrada de forma automática

En el escenario 1 todos los reportes se identifican en el mismo origen, el Resolver DNS. Con la instalación de las VA las petición llegan desde la máquina del cliente y se pueda reportar a la nube la IP de la máquina que realiza la petición.

Las resoluciones internas se seguirán realizando desde los DNS Resolver.



Esta instalación es más compleja que las dos anteriores.

Las VA necesitan:

- Dos máquinas virtuales, para tener alta disponibilidad, aunque valdría con una:
  - VMWare: Deploy VAs in VMware (umbrella.com)
  - HyperV: Deploy VAs in Hyper-V for Windows 2012 or Higher (umbrella.com)
- Datos importantes a configurar en las VAs:
  - IP de la red
  - IP del Resolver interno
  - Datos de los servidores de Umbrella.
- Hay que definir los dominios internos que que debe resolver el Servidor DNS, en ***Deployments>Domain Management>Add.***

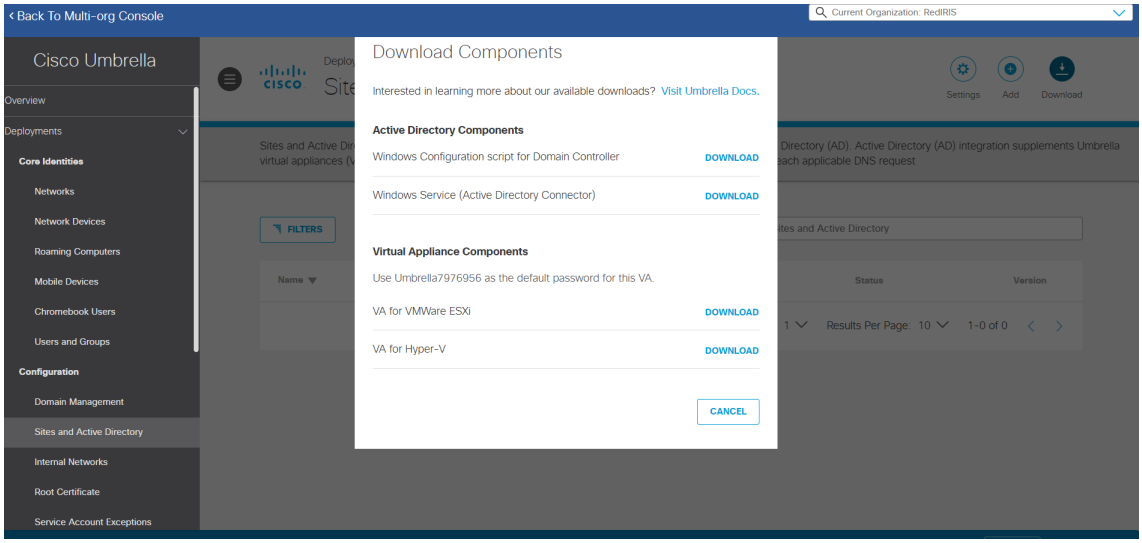
El AD connector. Es un elemento añadido a la arquitectura con VA. Instalando este elemento se reporta a la nube toda la información del usuario final.

El AD Connector se despliega:

- 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.

Con esta arquitectura las VA encaminaran la petición a la nube con toda la información de máquina y de usuario.

La descarga de las VA, el AD Connector y el script (opcional) necesarios para realizar esta instalación se hace en ***Deployments>Copre Identities> Sites and Active Directory:***



Para todo el despliegue es importante revisar que la comunicación entre los distintos elementos está permitida.

Documentación:

https://docs.umbrella.com/umbrella-user-guide/docs/introduction-4

Introduction (umbrella.com)

Cisco recomienda no dirigir el correo a Cisco Umbrella

La recomendación de Cisco es **no dirigir las peticiones DNS del correo hacia Cisco Umbrella**.

Según esta recomendación, cuando se configure el forwarding habría que diseñarlo de tal manera que el correo siga haciendo la resolución directamente contra el resolver de la institución, pero sin usar Cisco Umbrella.

Según Cisco, en el caso de encaminar el correo se podría comprometer su correcto funcionamiento. Esto se debe a que el filtrado de correo entrante genera múltiples resoluciones DNS y Umbrella podría introducir hasta 3 tipos de errores:

- **De seguridad**: Ocurriría cuando un dominio comprometido, que Umbrella categoriza como malicioso, envía un correo. Cuando Umbrella lo resuelve y ve que es malicioso lo bloquea y redirige a la página de bloqueo. No aporta seguridad adicional y elimina la capacidad de enviar y recibir desde/hacia dicho dominio. Además, interfiere en los procesos antispam que tratan de validar si el origen es auténtico, no si es malicioso. Umbrella en estos casos, al resolver la query, devuelve la página de bloqueo, es decir, una IP que no es la real, lo que puede impedir una validación y categorización correctas, y añade SPAM que probablemente no lo es.
- **De listas de bloqueo**: Si en el proceso de validar el correo, se hacen consulta DNS a ciertos servicios que publican su información vía DNS, puede suceder que dichas listas no respondan a Umbrella por su política de uso o volumen de consultas y directamente

no le responden. Aunque se tenga el Modo Transparente aplicado este tipo de consultas, no se resolverían y se comprometería el correcto funcionamiento del correo.

- **De contenido**: si se tiene un contenido bloqueado y Umbrella detecta correos con ese contenido puede bloquearlos y que no se reciban.

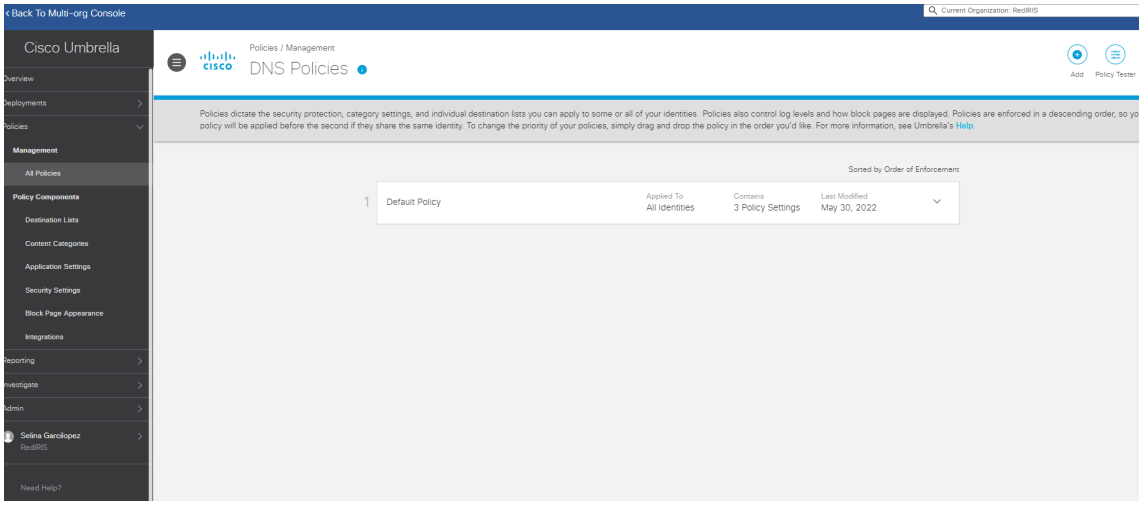
Configuración avanzada del servicio

Políticas de seguridad.

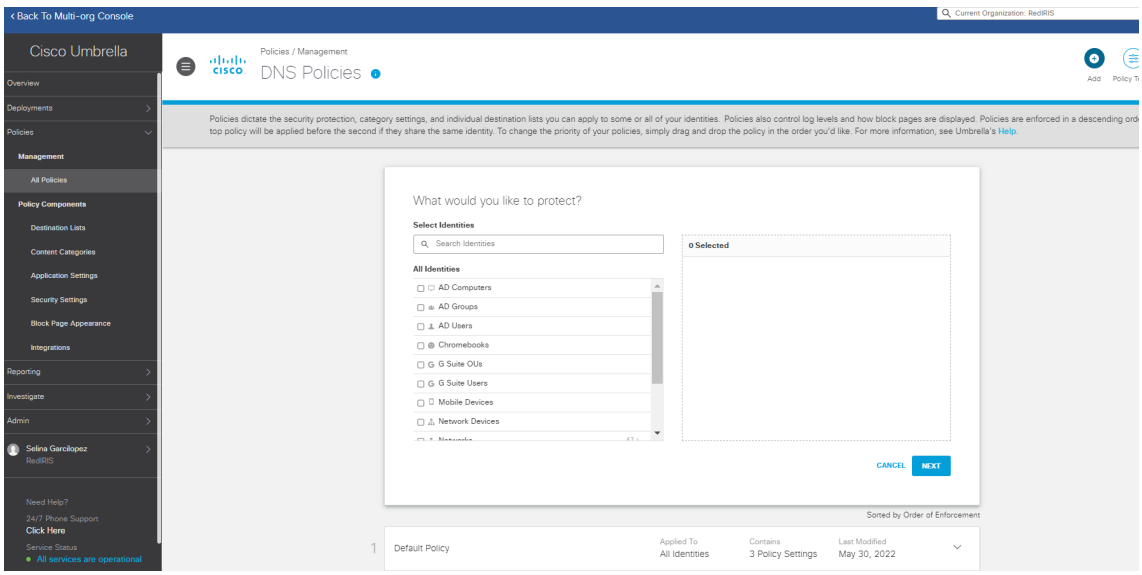
El tenant se entrega en Modo Transparente lo que implica que no hay seguridad aplicada.

Para subir el nivel de protección, según los criterios de seguridad de la propia organización hay que crear políticas de seguridad:

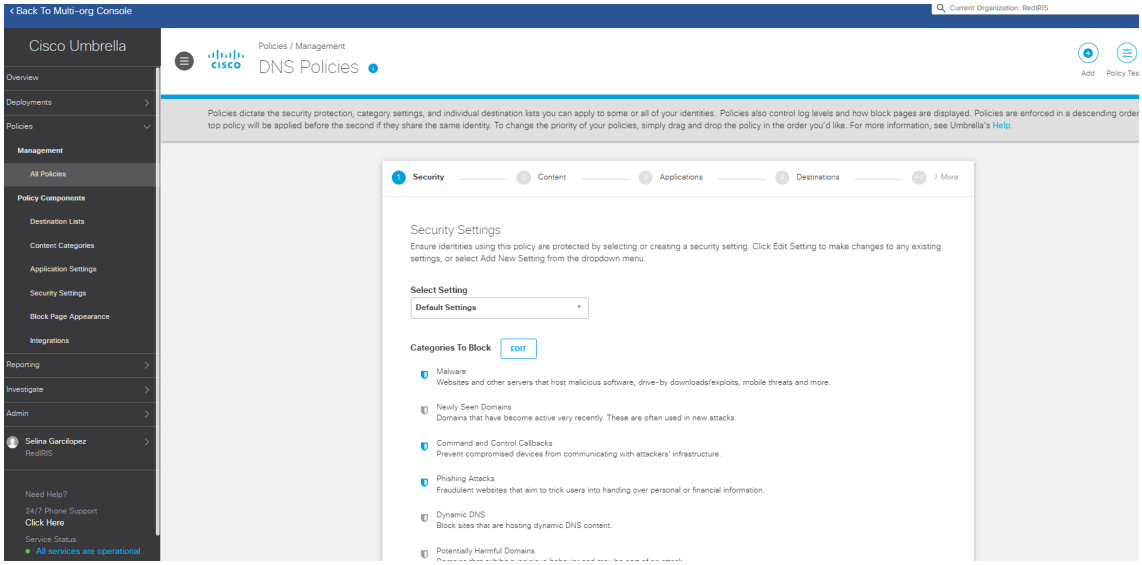
En ***Policies>Management>All Policies*** pulsar el botón ***Add.***



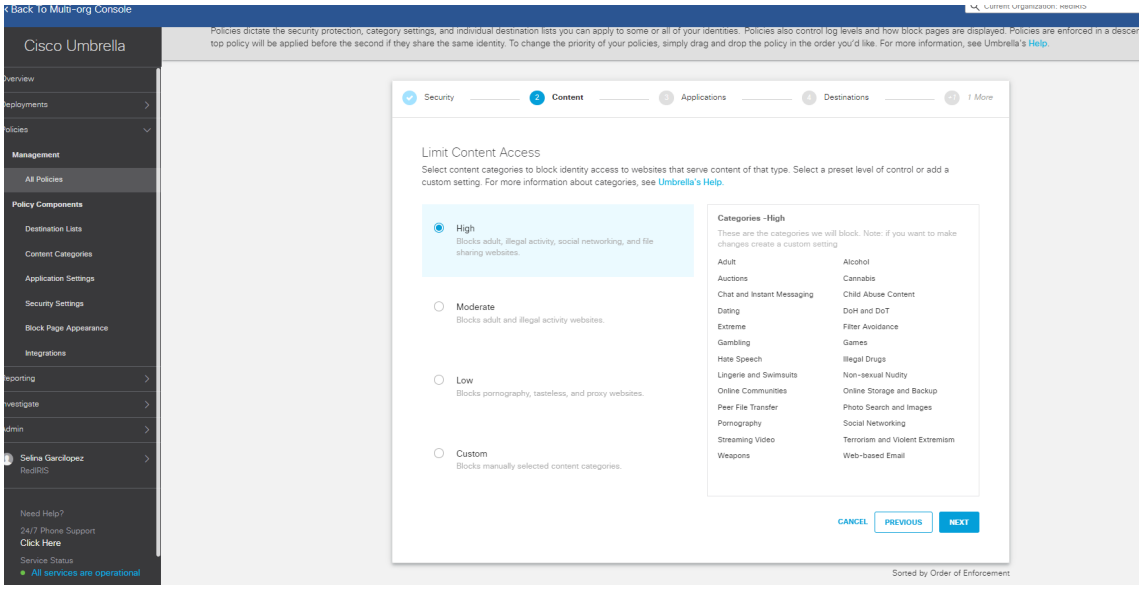
- Lo primero indicar sobre que parte de la red se va a aplicar la política.



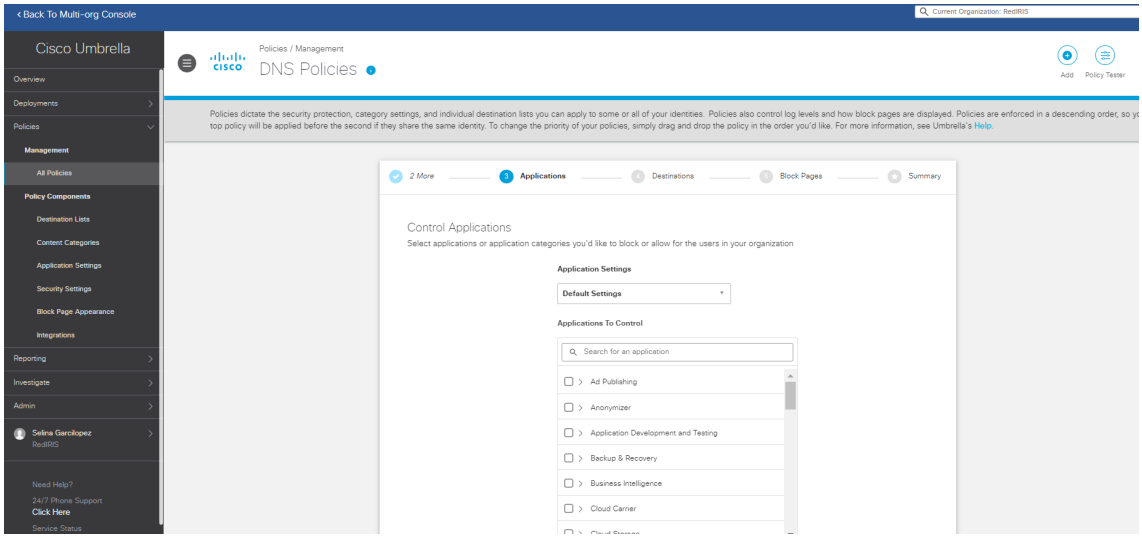
- Posteriormente decidir las acciones a tomar cuando se aplique la política y los criterios de seguridad que se van a aplicar:
    - Categorías:



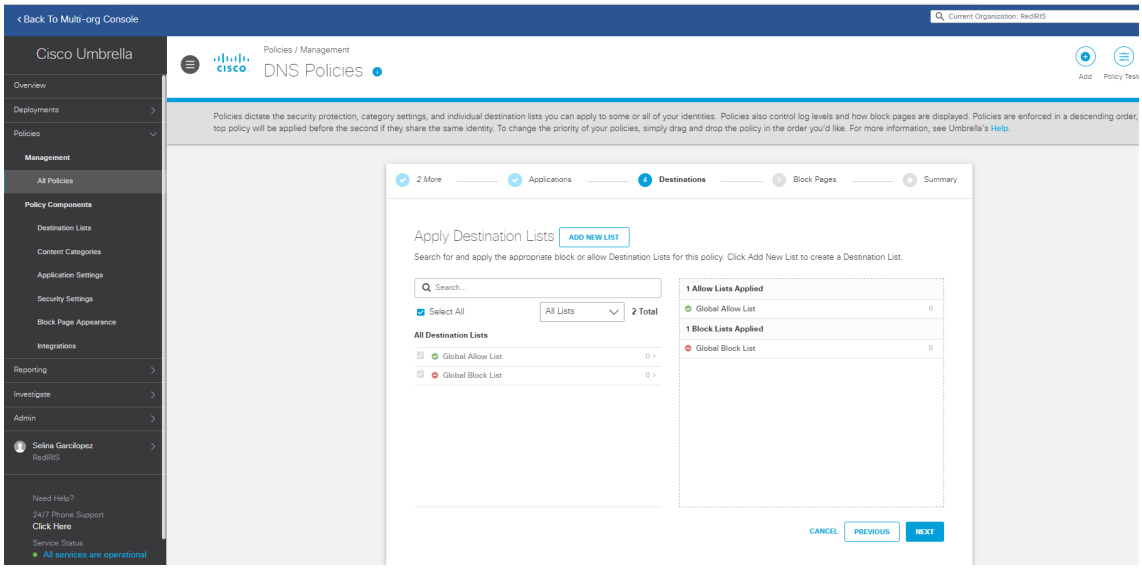
- Contenido



- Aplicaciones



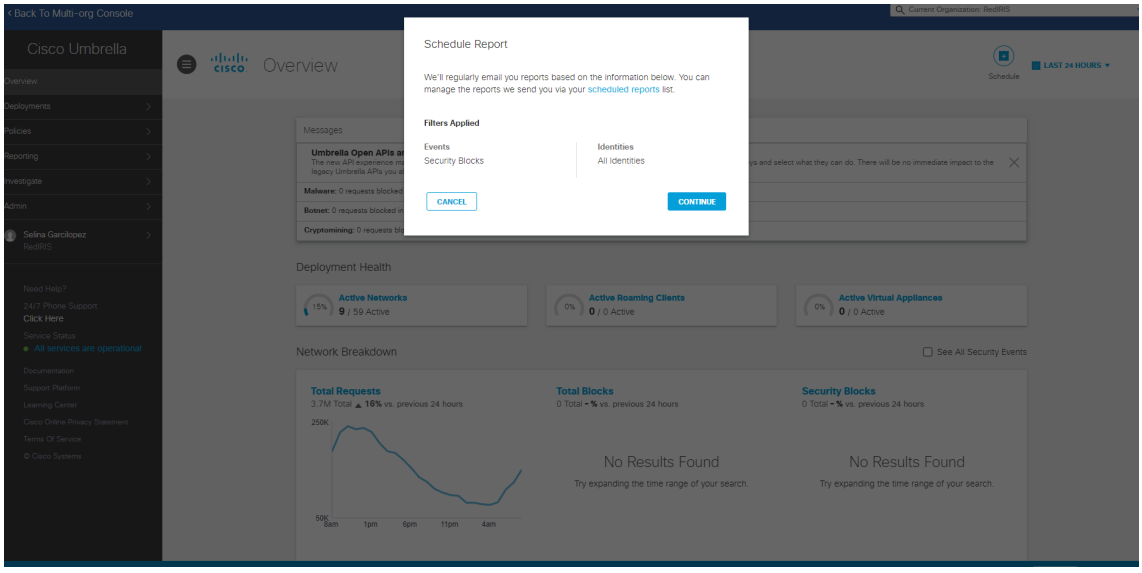
- Listas:



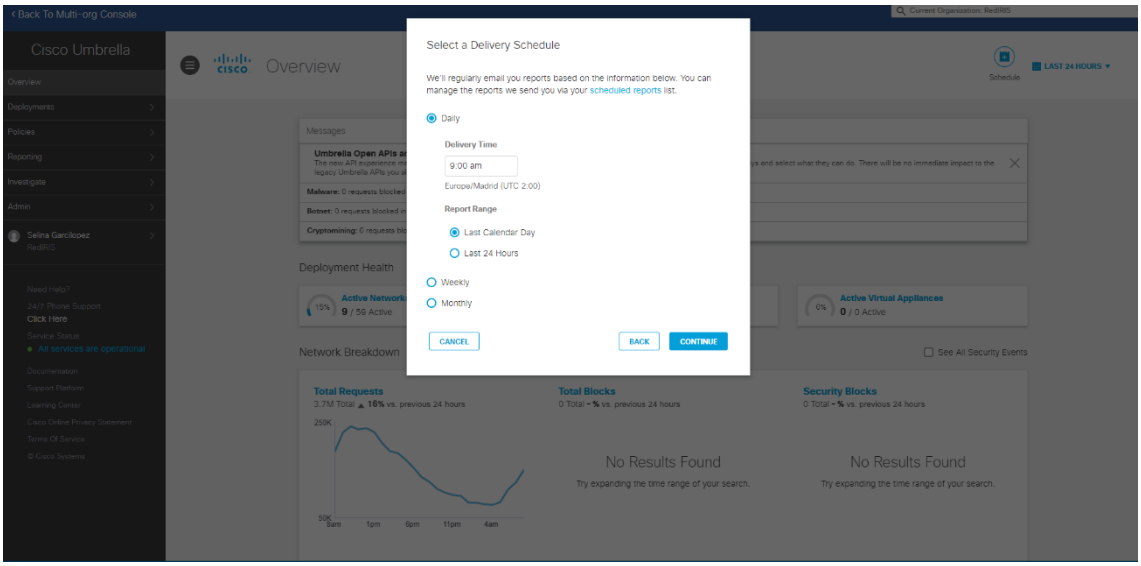
Lo que no se quiera aplicar se deja en blanco.

Informes de Uso. Reporting

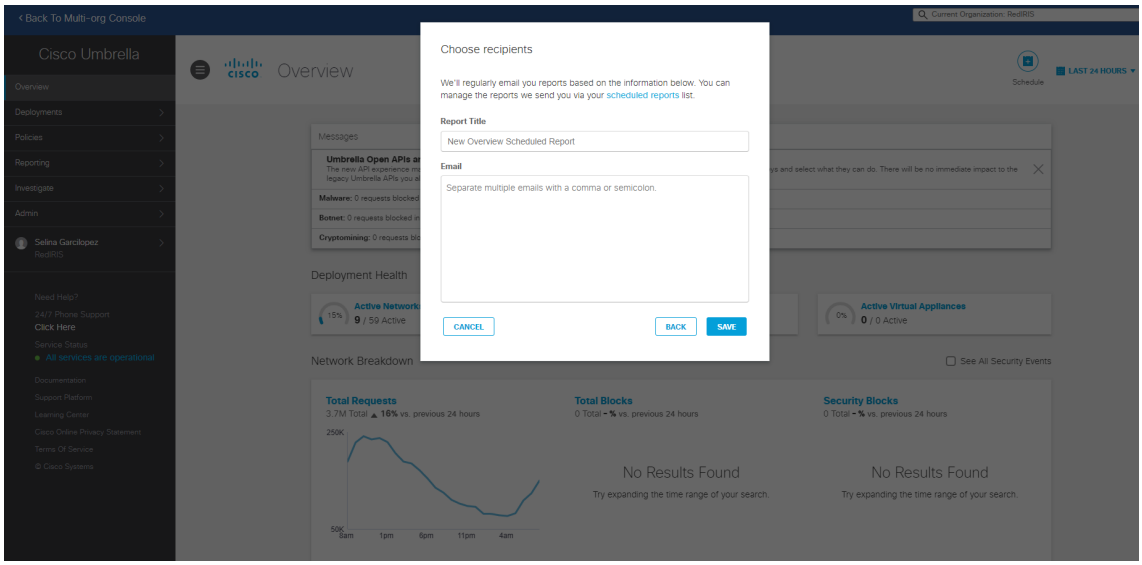
Se pueden generar informes programados que se reciban en el mail. El de mayor utilidad es el de los dominios bloqueados, para generar el reporte hay que ir a ***Overview> Botón de Scheduler***



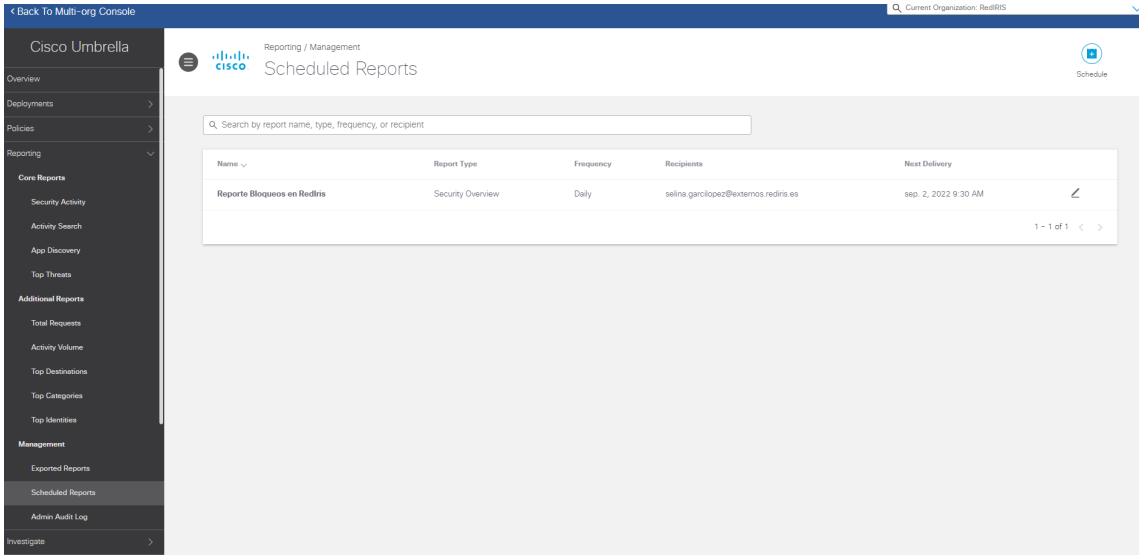
Seleccionar la periodicidad: diario, semanal o mensual. También el horario de envió del correo.



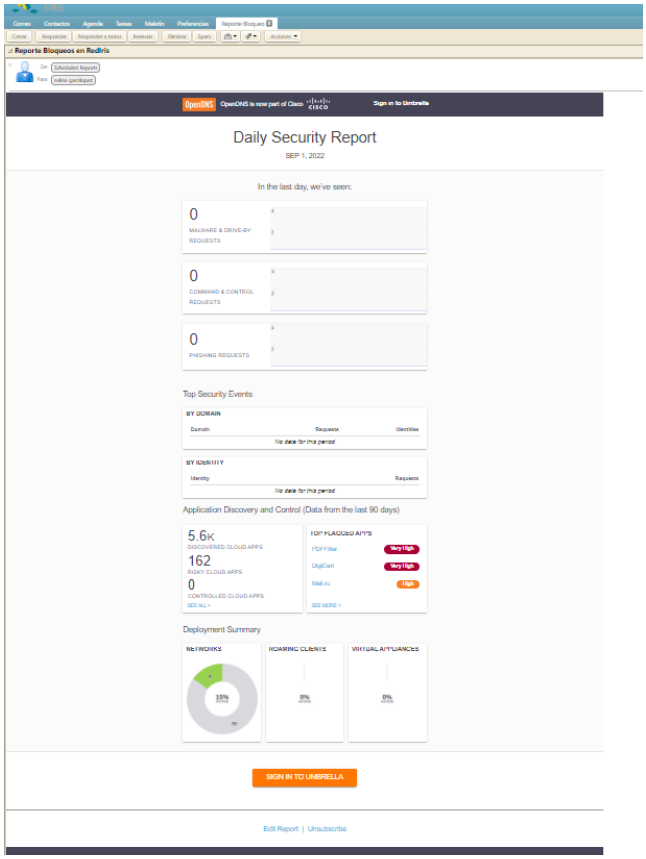
Se define el título del fichero del reporte, así como, el mail donde le queremos recibir los informes:



En ***Reporting>Management>Scheduled Report*** aparece el reporte creado y se puede editar.



El reporte se recibe por correo electrónico con el siguiente formato:



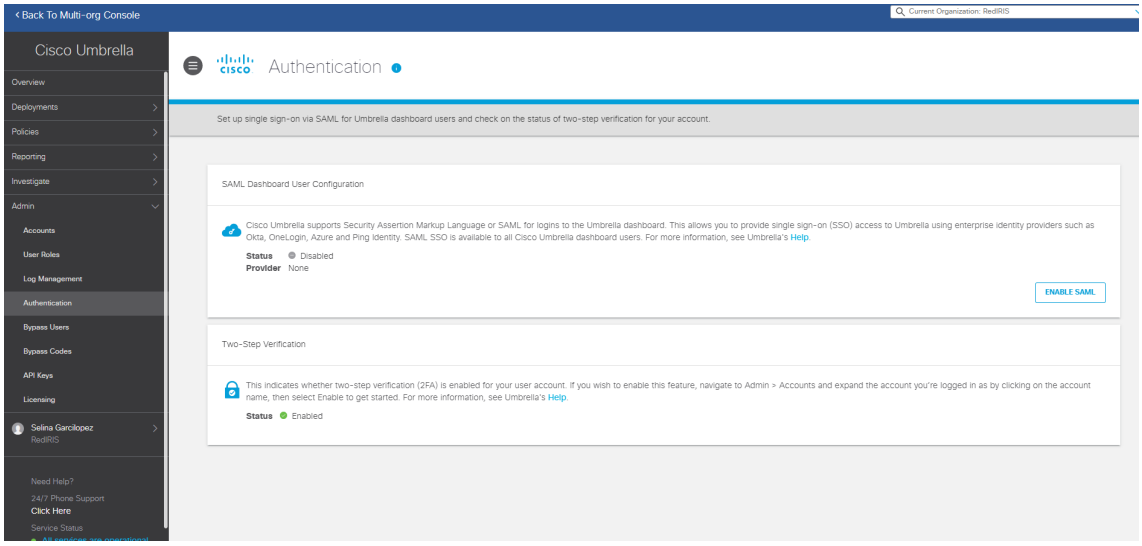
CISCO utiliza Sparkpost para enviar los correos. Algunos FW a nivel IPS podrían bloquear estos correos, o meterlos a spam. Nos recomiendan revisar los filtros de SPAM. Ya sea que la puerta de enlace del servidor de correo alojada localmente o en la nube, es probable que el correo electrónico se haya puesto en cuarentena en ese nivel. Umbrella envía sus informes desde: **scheduled-reports-feedback@opendns.com.**

Autenticación mediante SAML

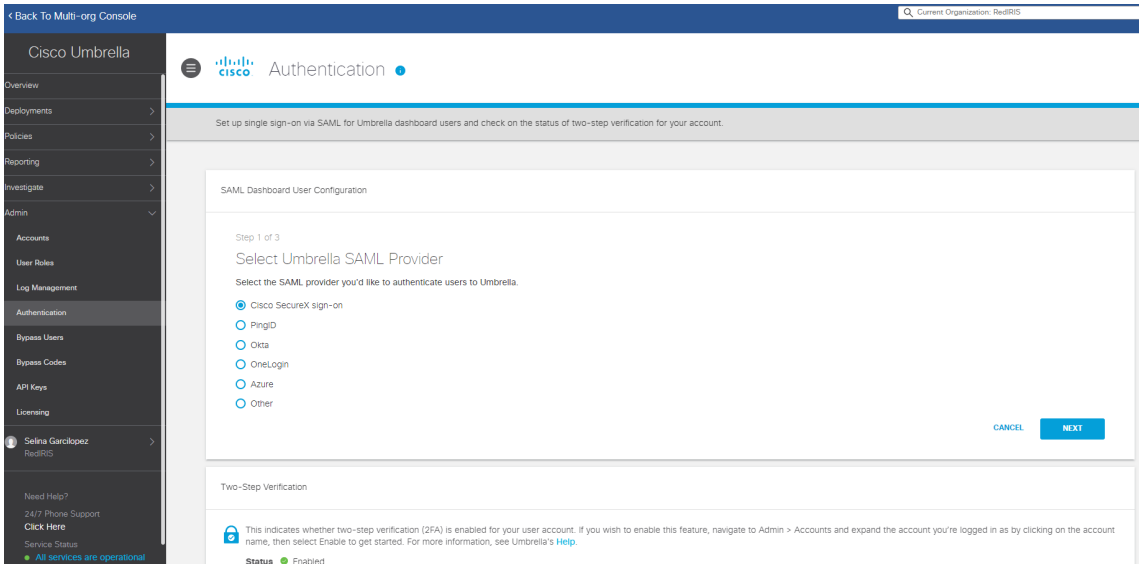
Sí, Cisco Umbrella permite autenticar los usuarios creados localmente en el tenant mediante consultas SAML al proveedor de identidad (idp) de la institución.

La configuración de SAML se hace *en* ***Admin>Authentication*****.**

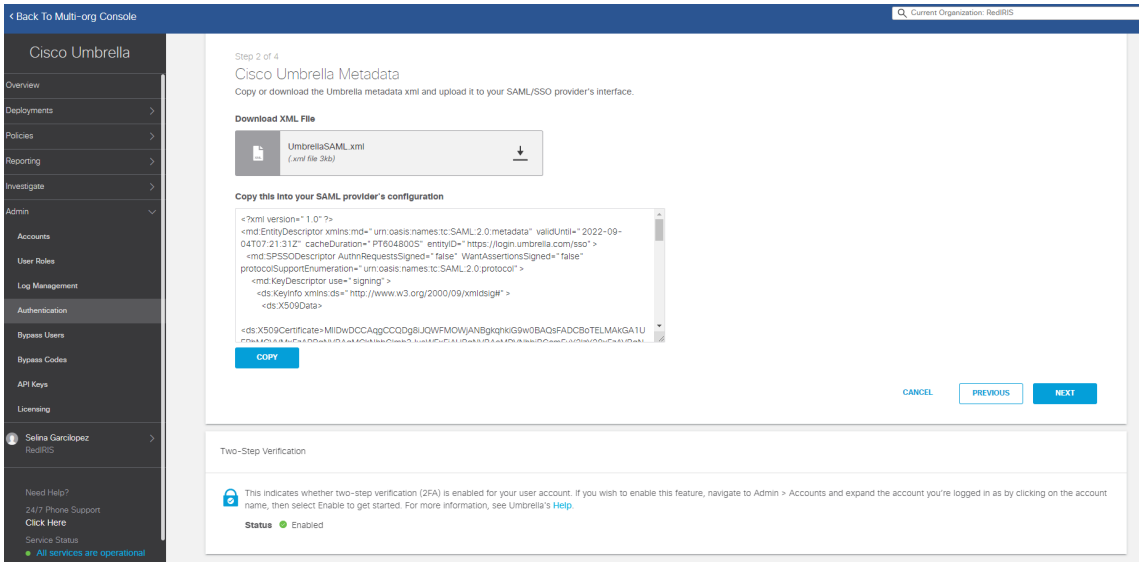
- ***Enable SAML*****.**
- Se selecciona el proveedor del servicio de autenticación:



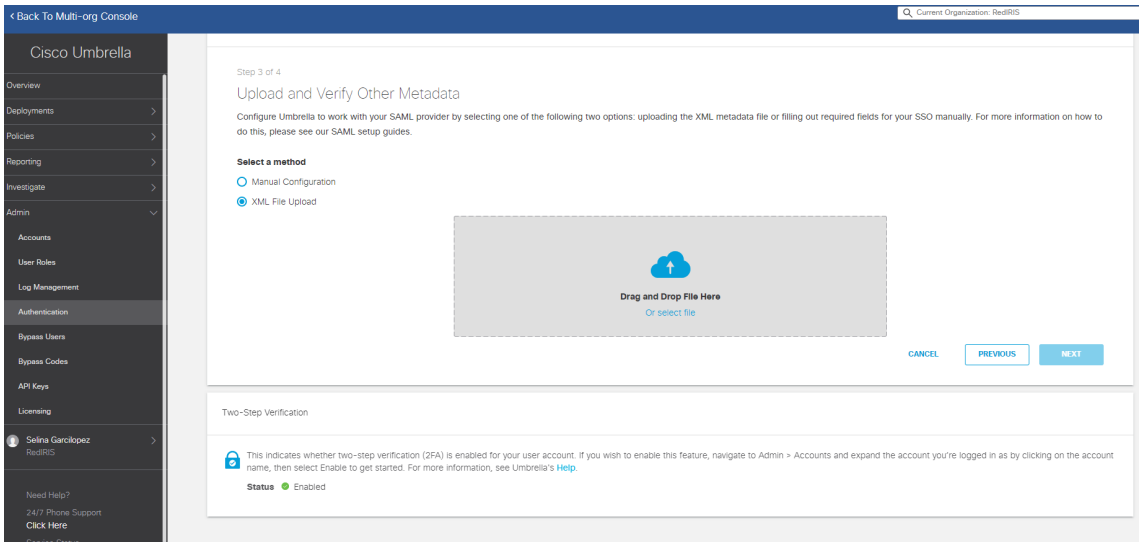
- Para configurar un proveedor propio de la organización seleccionar la opción **Other.**



- Descargar el fichero XML para proporcionárselo a proveedor del servicio:



- Hay dos opciones para configurar los datos del proveedor:
  - Cargar el fichero XML, que nos proporcione el proveedor del servicio.

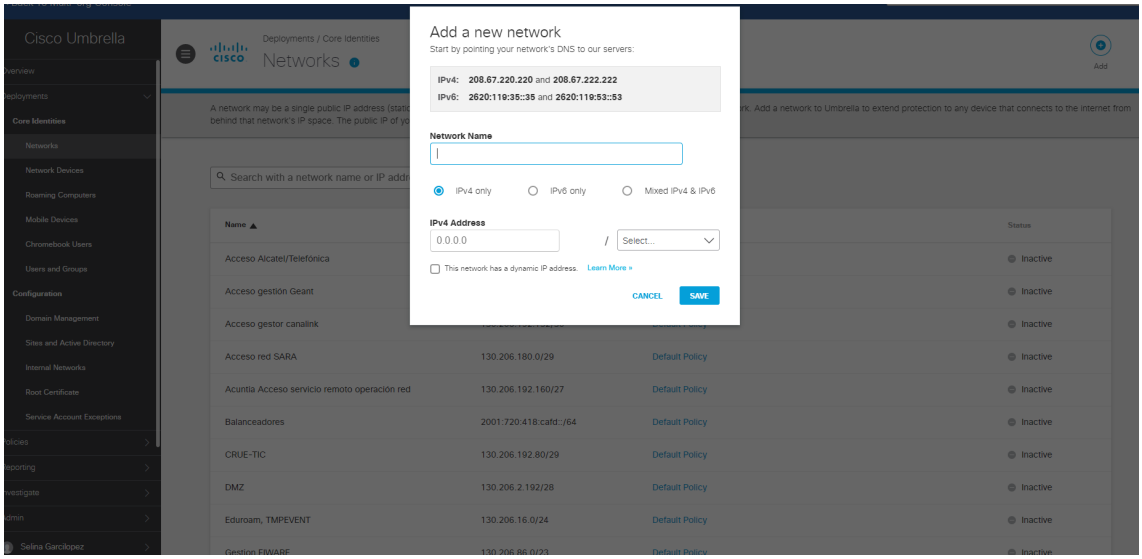


Modificación de las redes y/o mayor subnetting

El tenant se entrega configurado con la red o redes de la organización.

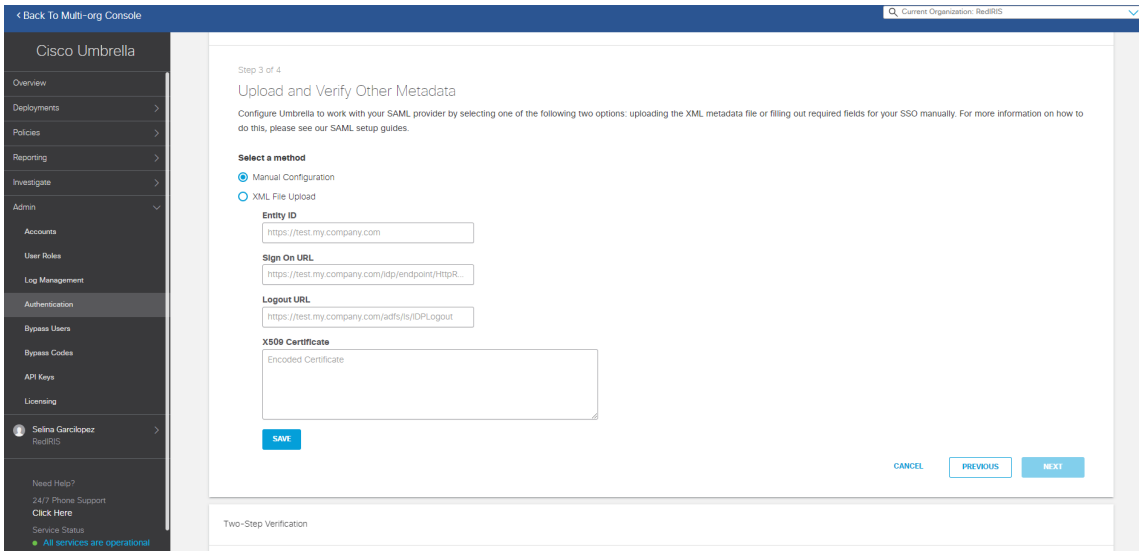
Si se quieren aplicar políticas diferentes según las redes que tenga la organización, se pueden hacer subnetting según las necesidades que tenga la propia organización.

Las redes se añaden en la **Deployments>Core Identities> Networks>Add**



Hay que añadir nombre de la red y direccionamiento.

- Realizar la configuración manual con los siguientes datos, que nos lo tiene que proporcionar el proveedor del servicio:



Preguntas frecuentes

¿Qué sucede al acabar las licencias que provee el servicio DNS Firewall de RedIRIS?

Cuando se acabe la licencia la organización tendrá 14 días para renovar o migrar a una organización con contracto. Si no se renueva la licencia, quedarán todas las redes y usuarios sin políticas. Solo se tendrá la resolución DNS de Umbrella.

¿Qué sucede si supero el número de licencias asignadas a mi tenant?

Si se está sobre utilizando la herramienta, el equipo de ventas de Cisco mandará un correo con un aviso, pero seguirán aplicándose las políticas sin problemas. Si la institución recibe algún aviso de ese tipo lo debe notificar a RedIRIS en dnsfirewall@rediris.es

¿Qué sucede si despliego agentes y cambian el DNS a mano?

Si el agente está activo, aunque cambies los DNS a mano en el SO no tendrá efecto, dado que el agente intercepta las peticiones y las redirige hacia Umbrella.

¿Qué sucede si tengo el agente activo y entro en la red interna?

El Roaming Client si se conecta a una red con despliegue de VA, por defecto se desactiva el agente. Para mantener el agente activo siempre, desactivar VA backoff. Si la red está protegida y el agente se mantiene activo, hay que tener cuidado con el orden de las políticas.

Si no hay despliegue de VA, no se desactivará automáticamente, habría que dimensionar bien las políticas, o desactivarlo al entrar en la red interna.

¿Qué sucede si mi institución está formada por múltiples sedes cada una con su arquitectura y su propio AD y desplegamos VAs?

En el dashboard de la institución hay que crear un SITE por cada sede. En cada sede se hará el despliegue de las VAs. Dentro del Dashboard en cada SITE hay que añadir las VAs y los AD de su sede.

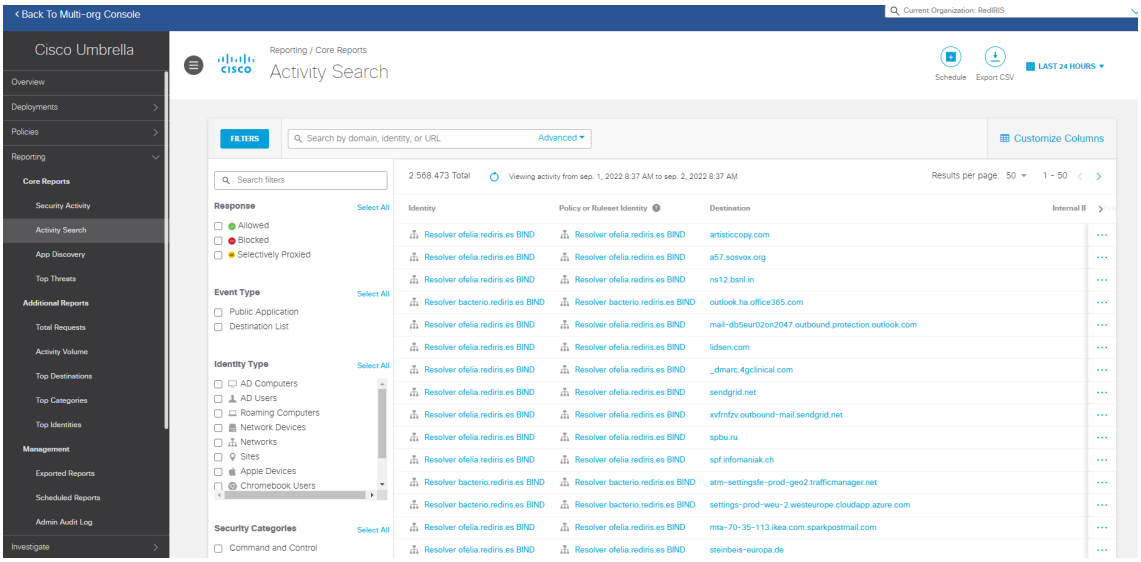
Se puede aplicar políticas a cada SITE.

https://docs.umbrella.com/deployment-umbrella/docs/multiple-active-directory-and-umbrella-sites

¿Como visualizar el tráfico DNS enviado a Umbrella?

Tanto el tráfico bloqueado como permitido se puede visualizar en ***Reporting>Core Reports>Activity Search.***

Se selecciona en el menú de la izquierda el tráfico que se quiere visualizar: el permitido el bloqueado, o ambos. Si no se selecciona ningún filtro sale todo el tráfico.



¿Qué sucede si mi organización tiene una protección DNS en el FW y despliega UMBRELLA?

Umbrella es complementario a la protección ya aplicada. Primero se aplicaría la protección establecida en el FW y luego la protección del FW DNS de UMBRELLA.

Sería una protección añadida a la que ya se tiene desplegada.

¿Las IPs de las páginas de bloqueo son siempre las mismas?

Las páginas de bloqueo son diferentes dependiendo de la categoría. En el siguiente enlace se muestran el listado:

https://support.opendns.com/hc/en-us/articles/227986927-What-are-the-Cisco-Umbrella-Block-Page-IP-Addresses-