

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

Versión 1.10 - 13/04/2023

Que es un DNS Firewall	3
Servicio DNS Firewall de RedIRIS	3
Plataforma del servicio	3
Servicio de administración y soporte	4
Solicitud de alta en el servicio	4
Configuración inicial del servicio	4
Despliegue de la herramienta	6
Configurar el DNS Resolver hacia Cisco Umbrella	<b>6</b>
PowerDNS	7
Microsoft	7
	9
Despliegue de agentes en los clientes	13
Instalación de Virtual Appliances.	14
Cisco recomienda no dirigir el correo a Cisco Umbrella	16
Configuración avanzada del servicio	17
Políticas de seguridad	17
Informes de Uso. Reporting	19
Autenticación mediante SAML	23
Modificación de las redes y/o mayor subnetting	24
Preguntas frecuentes	26
¿Qué sucede al acabar las licencias que provee el servicio DNS Firewall de RedIRIS? _	26
¿Qué sucede si supero el número de licencias asignadas a mi tenant?	26
¿Qué sucede si despliego agentes y cambian el DNS a mano?	26
¿Qué sucede si tengo el agente activo y entro en la red interna?	26



¿Qué sucede si mi institución está formada por múltiples sedes cada una con su	
arquitectura y su propio AD y desplegamos VAs?	26
¿Como visualizar el tráfico DNS enviado a Umbrella?	28
¿Qué sucede si mi organización tiene una protección DNS en el FW y despliega	
UMBRELLA?	28



## 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 <u>DNS Firewall</u> 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 <u>DNS Security for Education</u>, 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.
  - o Contacto vía correo electrónico a dnsfirewall@rediris.es
- Atención de incidencias 24x7 para incidencias:
  - Contacto vía correo electrónico a <u>dnsfirewall@rediris.es</u> 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: <u>umbrella-</u> <u>support@cisco.com</u>.

## Configuración inicial del servicio

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

- <u>Modo transparente</u>: 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*:

Reporting ~										
Core Reports	Q. Search filters		2.314.343 Total 👌 Viewing acti	ity from jul. 27, 2022 12:05 PM to jul. 28, 20	22 12:05 PM		Res	sults per page:	50 - 1 -	- 50 <
Security Activity	Response	Select All	Identity	Policy or Ruleset Identity	Destination	Internal IP	External IP	DNS Type	Action	Categ
Activity Search	O Allowed     O Allowed     O Allowed		A Resolver ofelia.rediris.es BIND	A Resolver ofelia.rediris.es BIND	arin-innovation.com		2001:720:418:caf1::19	DS	Allowed	Busine
App Discovery	Selectively Proxied		A Resolver ofelia.rediris.es BIND	A Resolver ofelia.rediria.es BIND	arininnovation-com01b.mail.protection.outlook.com		2001:720:418:caf1::19	A	<ul> <li>Allowed</li> </ul>	Softw
Top Threats	Front Ton 1		A Resolver ofelia rediris.es BIND	A Resolver ofelia.rediris.es BIND	guise		130.206.1.19	MX	<ul> <li>Allowed</li> </ul>	Educa
Additional Reports	Public Application	Select All	$\underline{\mathbb{T}}_{1}$ Resolver of elia rediris.es BIND	A Resolver ofelia.rediris.es BIND	133.0.107.40.zen.spamhaus.org		130.206.1.19	А	<ul> <li>Allowed</li> </ul>	Softwa
Total Requests	Destination List		A Resolver ofelia.rediris.es BIND	A Resolver ofelia.rediris.es BIND	40.107.237.85_i.jci.com_d.espf.agari.com		130.206.1.19	A	<ul> <li>Allowed</li> </ul>	Comp
Activity Volume		_	🚠 Resolver ofelia.rediris.es BIND	A Resolver ofelia.rediris.es BIND	133,147,157,211,sbl.spamhaus.org		130.206.1.19	A	Allowed	Softwa
Top Destinations	Identity Type	Select All	A Resolver ofelia rediris es BIND	A Resolver ofelia.rediris.es BIND	178.76.54.207.in-addr.arpa.eu.iphmx.com		2001:720:418:caf1::19	PTR	Allowed	Infrast
Top Categories	AD Users	Â.	A Resolver ofelia.rediris.es BIND	A Resolver ofelia.rediris.es BIND	advice.3.pro-bridging.co		130.206.1.19	А	<ul> <li>Allowed</li> </ul>	Uncat
Top Identities	Roaming Computers     Network Devices		A Resolver ofelia.rediris.es BIND	A Resolver ofelia.rediris.es BIND	digi-218.searchdigital.space		130.206.1.19	A	<ul> <li>Allowed</li> </ul>	Uncati
Management	A Networks		A Resolver ofelia.rediris.es BIND	A Resolver ofelia.rediris.es BIND	transmail.net		2001:720:418:caf1::19	DS	Allowed	Webrr
Exported Reports	Sites     Apple Devices     G Chromebook Users		A Resolver ofelia rediris.es BIND	A Resolver ofelia.rediris.es BIND	spf.zoho.com		130.206.1.19	TXT	<ul> <li>Allowed</li> </ul>	Portals
Scherbileri Darvete		•	A Resolver ofelia rediris.es BIND	A Resolver ofelia.rediris.es BIND	prda.aadg.msidentity.com		130.206.1.19	AAAA	<ul> <li>Allowed</li> </ul>	Infrast
A deale Availad an			A Resolver bacterio.rediris.es BIND	A Resolver bacterio.rediris.es BIND	login.live.com		2001:720:418:cafe::250	A (	<ul> <li>Allowed</li> </ul>	Search
Admin Addit Log	Security Categories	Select All	A Resolver ofelia.rediris.es BIND	A Resolver ofelia.rediris.es BIND	usp-ceu-es.mail.protection.outlook.com		130.206.1.19	AAAA	<ul> <li>Allowed</li> </ul>	Softwa
Investigate >	Command and Control		A Resolver ofelia.rediris.es BIND	A Resolver ofelia.rediris.es BIND	ns1.globalconferences2.org		130.206.1.19	AAAA	<ul> <li>Allowed</li> </ul>	Uncab

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

Back To Multi-org Console					٩	Current Organization: CSX
Cisco Umbrella	Palicies / Palicy Com	ponents				
erview	Security S	etungs				
ployments >						
icies 🗸 🗸		Q, Search				
Management All Policies		Centralized Default Settings	Settings Enabled 3	Integrations 0	Last Modified Jun 21, 2022	~
Policy Components Descination Lists		Default Settings	Settings Enabled 3	Integrations 0	Last Modified Jul 27, 2022	~
Content Categories		Modo Transparente	Settings Enabled 0	Integrations 0	Last Modified Jun 27, 2022	~
Security Settings						
Block Page Appearance Integrations						
xorting >						
szigote >						
nin >						
Selina Garcilopez > CRC						
Need Help?						
Click Here						



## 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:



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:



• 🕪   📶 👗 🛄	🔍 🗃   🚺 🖬   📕				
> 192.168.66.9 > EDNSPRIVW01	EDNSPRIVW01 Propertie	es		? ×	<
EDNSPRIVW02	Debug Logging	Even	it Logging	Monitoring	
	Interfaces	orwarders	Advanced	Root Hints	
	IP Address 208.67.222.222 208.67.220.220 ✓ Use root hints if no Note: If conditional for be used instead of serv forwarders, navigate to tree.	forwarders an warders are d ver-level forwa o the Condition	Server FQON resolver 1.opendn resolver 2.opendn e available efined for a given d arders. To create of all forwarders not	s.com s.com Edit omain, they will r view conditional e in the scope	

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

Interfaces	Ferry	- daha	Advanced		Deet Linte
Debug Logging	FORW	arue	Auvanceu	M	ROOL HILLS
Debug bogging	' I	Event	Logging	M	onitoring
To assist with debu	ugging, y	you can reco	ord the packets se	ent and	d received
V log packata for	debugg	ine. Debug	logging is disable	u by u	erduit.
<ul> <li>Log packets for</li> <li>Dacket direction:</li> </ul>	uebugg	in ig	Transport prote	col:	
	)	a a la at a t		),001	anlast -t
	- }	least one		- }	least one
			e rer		
acket contents:			Packet type:	•	
V Queries/Transf	ers )	select at	✓ Request	- {	select at
✓ Updates	Ś	least one	Response	,	least one
Notifications	, r				
Other options:					
Log unmatched	incomin	g response (	packets		
Details					
Filter packets b	y IP add	iress	Filter		
Log file					
File path and na	me:	L:\logs\dns	\dnslog1.log		
-	L		$\neg$		
Maximum size (b	ytes):	500000000			

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:

 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.



Toggle Basic Mode	Basic	
General		
Forwarders	FORWARDERS	+ 1 🗰
Updates	Addresses	
Queries	208 67 222 222	1
Zone Transfers		
Root Name Servers	208.67.220.220	
Sort List	2620:119:35::35	
Blackhole	2620:119:53::53	
Logging		
Host Naming		
GSS-TSIG		
DNSSEC		
Blacklist	Use Forwarders Only	
UNS64	Add client IP, MAC addresses, and DNS View name to outgoing recursive queries	
Restart	Copy client IP, MAC addresses, and DNS View name to outgoing recursive queries	
Security		
DNS Scavenging		
Traffic Control		

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.

Basic
Negative-caching TTL 15 Minutes
Primary name server (for SOA MNAME field)
Serial number 419 Inherited from Member
Serial number 419
Different serial numbers for each master is normal.
Email address (for SOA RNAME field)

#### EfficientIP

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

#### 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
    iLl 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.dBbb 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 l.l.l). Copyright 1996-2005 Kunihiro Ishiguro, et al. dns-anycast-l#
- 3. 3. Run the following command to display info on IS-IS neighbor:

dns-any	cast-1# show i	isis neighbor					
Area 18	SIS_0:	Teberfree			N=1463==	CMDA	
ayace	im TO	inceriace	L state		Horacime	SNEA	
route	er .	em3		1 Up		8	ca01.025d.0000
dns-any	cast-1# show i	isis hostname					
Level	System ID	Dynamic Host	name				
1	1720.1600.1001	l router					
*	1720 1600 2003	dos-anvcast-	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<sup>2</sup>.

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.
- 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 <u>CREATE</u>. 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 IDNS > 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 E. 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.
- Click on OK to complete the operation. The report opens and closes. The properties page refreshes and displayed the new settings.
- Repeat step c to i for each server or smart architecture on which you plan to deploy DNSCrypt. i.

#### 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

Retrieve your DNSCrypt parameters using the script umbrella\_setup. You must specify C. 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 {
 edma-opendma yes;
 edma-opendma-organization-ID>;
 edma-opendma-organization-ID>;
 edma-opendma-deviceid "<your-Cisco-Umbrella-Device-ID>";

- d. Copy the lines returned.
- Edit the DNS alobal include file. e.
  - 1. Open the /datal/etc/namedb/global include.conf.
  - Copy the lines of the DNSCrypt global parameters your retrieved.





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  ${\tt server}$  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 <u>https://docs.umbrella.com/umbrella-user-guide/docs/download-and-install-the-roaming-client</u>

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:
  - o VMWare: Deploy VAs in VMware (umbrella.com)
  - o 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:* 

< Back To Multi-org Console				Q Current Organization: RedIRIS
Cisco Umbrella	Deplo	Download Components		* • 1
Overview	cisco. Site	Interested in learning more about our available downloads? Visit L	Jmbrella Docs.	Settings Add Download
Deployments ~	Sites and Active Di	Active Directory Components		Disastes (AD), Active Disastes (AD) integration supplements Undersity
Core Identities	virtual appliances (	Windows Configuration script for Domain Controller	DOWNLOAD	each applicable DNS request
Networks		Windows Service (Active Directory Connector)	DOWNLOAD	
Network Devices	FILTERS			ites and Active Directory
Roaming Computers		Virtual Appliance Components		
Mobile Devices	Name 🔻	Use Umbrella7976956 as the default password for this VA.		Status Version
Chromebook Users		VA for VMWare ESXi	DOWNLOAD	1 V Results Per Page: 10 V 1-0 of 0 < >
Users and Groups		VA for Hyper-V	DOWNLOAD	
Configuration				
Domain Management			CANCEL	
Sites and Active Directory				
Internal Networks				-
Root Certificate				
Service Account Exceptions				

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.

< Back To Multi-org Console								Q Current Organiza	Jon: RedIRIS	
Cisco Umbrella		Policies / Management							(	•
Dverview		DINS POlicies							1	Add Policy Tester
Deployments >	Palision	distate the security protection, extend	nu pattings, and individual doctination lists up	u can annlu to como or all of	ugur identition Polici	os also control log loval	and haw black pages as	o displayed Policies are	onformed in a dense	odioa ordar, co ua
Policies 🗸 🗸	policy w	ill be applied before the second if the	/ share the same identity. To change the prio	prity of your policies, simply d	rag and drop the polic	y in the order you'd like	. For more information, se	e Umbrella's Help.		noing order, so yo
Management										
All Policies							Sorted by Order	of Enforcement		
Policy Components		1	Default Policy		Applied To All Identities	Contains 3 Policy Settings	Last Modified May 30, 2022	~		
Destination Lists						o roney coungo	1107 00, 2022			
Content Categories										
Application Settings										
Security Settings										
Block Page Appearance										
Integrations										
Reporting >										
nvestigate >										
Admin >										
Selina Garcilopez > RedIRIS										
Need Help?										

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

< Back To Multi-org Console			<mark>ି ପ୍ରା</mark>	rrent Organization: RedIRIS
Cisco Umbrella	Policies / Management			<b>o</b> (#
Overview	UNS POlicies	•		Add Policy Tr
Deployments >	Deficies discussion and a second		identities Defining the second has been been been been as a second	and Onticipation and the descending and
Policies 🗸	top policy will be applied before the second	gory settings, and individual destination lists you can apply to some or all of yo if they share the same identity. To change the priority of your policies, simply	drag and drop the policy in the order you'd like. For more information, see U	norden policies are enforced in a descending ord- mbrella's Help.
Management				
All Policies				
Policy Components		What would you like to protect?		
Destination Lists		Select Identities		
Content Categories		Q. Search Identities	0 Selected	
Application Settings		All Identities		
Security Settings		AD Computers		
Block Page Appearance		□ ± AD Users		
Integrations		G Chromebooks		
Reporting >		G G Suite OUs		
Investigate >		G G Suite Users		
Admin		Mobile Devices		
Selina Garcilopez >		C. T. Maturela.		
RedIRIS			CANCEL NEXT	
Manual Marka 2				
24/7 Phone Support			Sorted by Order of Enforce	ment
Service Status All services are operational	1	Default Policy App	lied To Contains Last Modified dentities 3 Policy Settings May 30, 2022	

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



< Back To Multi-org Console	Q. Carrent Or	janization: RedIRIS
Cisco Umbrella	Policies / Management	• =
Overview	UNS POlicies	Add Policy Tes
Deplayments >	Deliniae distate the security presention extension extension and individual destination late usures and uto extra or all of usur identitias. Deliniae step control for lauses and how block names are disclosed. Del	rias are enforced in a descending order
Policies 🗸 🗸	top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. For more information, see Umbrella	s Help.
Management		
All Policies	0 Security O Content O Applications O Destinations O 1 More	
Policy Components		
Destination Lists	Security Settings	
Content Categories	Ensure identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any existing	
Application Settings	serings, o seect koo ver sering non ne orgoown neno.	
Security Settings	Select Setting	
Block Page Appearance	ueraun Settings *	
Integrations	Categories To Block EDIT	
Reporting >	0 Malware	
Investigate >	websites and other servers that nost malicious sortivare, only-by downloads(exploits, mobile threats and more.	
Admin >	IV Newly Seen Domains Domains that have become active very recently. These are often used in new attacks.	
Selina Garcilopez > RedIRIS	<ul> <li>Command and Control Calibacia</li> <li>Prevent congromised devices from communicating with attackers' infrastructure.</li> </ul>	
Need Help?	<ul> <li>Phinking Attacks</li> <li>Fraudulent websites that aim to brick users into handing over personal or financial information.</li> </ul>	
24/7 Phone Support Click Here	Dynamic DNS     Block sites that are housing dynamic DNS content.	
<ul> <li>All services are operational</li> </ul>	Potentially Hermful Domains	

o Contenido

< Back To Multi-org Console						Current Organization: Redikts
Cisco Umbrella	Policies dictate the security protection, category s top policy will be applied before the second if the	ettings, and y share the	d individual destination lists you can apply to some or all of your in same identity. To change the priority of your policies, simply drag	dentities. Policies also control lo g and drop the policy in the orde	g levels and how block pages are dis r you'd like. For more information, see	played. Policies are enforced in a descer e Umbrella's Help.
Dverview						
Veployments >	•	Security	y 2 Content 3 Applica	ations Oe	estinations 0 1 h	fore
Policies $\sim$						
Management		Limit	Content Access			
All Policies		Select of custom	content categories to block identity access to websites that serve setting. For more information about categories, see Umbrella's F	e content of that type. Select a p lelp.	reset level of control or add a	
Policy Components				Categories -High		
Destination Lists		۲	High Blocks adult, illegal activity, social networking, and file	These are the categories we will changes create a custom settin	il block. Note: if you want to make	
Content Categories			sharing websites.	Adult	Alcohol	
Application Settings				Auctions Chat and Instant Messaging	Cannabis Child Abuse Content	
Security Settings			Moderate Blocke adult and Banal activity waheitee	Dating	DoH and DoT	
Block Page Appearance			unoone source one mogen evering meances.	Extreme Gambling	Filter Avoidance Games	
Integrations				Hate Speech	Illegal Drugs	
leporting >			Low Blocks pornography, tasteless, and proxy websites.	Lingerie and Swimsuits Online Communities	Non-sexual Nudity Online Storage and Backup	
ivestigate >				Peer File Transfer	Photo Search and Images	
idmin >				Streaming Video	Social Networking Terrorism and Violent Extremism	
Selina Garcilopez > RedIRIS			Custom Blocks manually selected content categories.	Weapons	Web-based Email	
Need Help? 24/7 Phone Support <b>Click Here</b>					CANCEL PREVIOUS NEXT	
Service Status     All services are operational					Sorted by Order of Enfo	rcement

• Aplicaciones

< Back To Multi-org Console	Q, Current	Organization: RedIRIS
Cisco Umbrella	Policies / Management	<ul> <li>(a) (a)</li> </ul>
Overview	CISCO. DNS Policies •	Add Policy Tester
Deployments >		
Policies $\checkmark$	roucies dictate the security protection, category security, and manufacturinals you can apply to some or an of your demotes. Forches also control log levels and now dock pages are displayed in top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. For more information, see Umbre	rolicies are enforced in a descending order, so yc lla's Help.
Management		
All Policies	📀 2 More 🔕 Applications 🔕 Destinations 💿 Block Pages 💿 Summary	
Policy Components		
Destination Lists	Control Applications	
Content Categories	Select applications or application categories you'd like to block or allow for the users in your organization	
Application Settings	Application Settings	
Security Settings	Default Settings v	
Block Page Appearance	Analizations To Control	
Integrations		
Reporting >	Q. Search for an application	
Investigate >	> Ad Publishing	
Admin >	> Anonymizer	
Selina Garcilopez      Audulos	> Application Development and Testing	
Redircis	> Backup & Recovery	
Need Help?	> Business Intelligence	
24/7 Phone Support Click Here	Cloud Carrier	
Service Status		



o Listas:

< Back To Multi-org Console		Q Current Organization: RedIRIS
Cisco Umbrella	Policies / Maragement	•
Overview		Add Policy Teso
Deployments >	Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages	are displayed. Policies are enforced in a descending order,
Policies 🗸	top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. For more informat	ion, see Umbrella's Help.
Management		
All Policies	🕑 2 More 🕑 Applications 🔕 Destinations 💿 Block Pages 💿	Summary
Policy Components		
Destination Lists	Apply Destination Lists and NEW LIST	
Content Categories	Search for and apply the appropriate block or allow Destination Lists for this policy. Click Add New List to create a Destination List.	
Application Settings		
Security Settings	Q Search 1 Allow Lists Applied	
Block Page Appearance	Select All All LISts V 2 Total 1 Block Lists Applied	
Integrations	All Destination Lists	0
Reporting >	Global Block List 0	
Investigate >		
Admin >		
Selina Garcilopez > RedIRIS		
Need Help?		
24/7 Phone Support Click Here Service Status All services are operational	CANCEL PREVIOUS	NEXT

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* 

< Back To Multi-org Console					Q Current Organization: RedIRIS	_
Cisco Umbrella	<b>e dudu</b> Ove	erview	Schedule Report We'll regularly email you repor manage the reports we send	ts based on the information below. You can you via your scheduled reports list.	Schedule	LAST 24 HOURS 🔻
Backymens > Nolces > Riconng > Investigate > Ramn > Solan Crustioner >		Messages Untrella Open APIs a The new API expenses m legacy Untrella APIs you a Malware: Crequests blocked Botne: Crequests blocked in Cryptomining: Crequests Mi	Filters Applied Events Security Blocks	Identities All Identities	$_{\rm H}$ and latter what they can do. There will be no investigate impact to the $~~\times$	
RedRes         Need Help?           24/7 Phone Support         Click Here           Service Status         • All services are operational		Deployment Health		Active Reaming Clients	Active Virtual Appliances     O / 0 Active     Gee All Security Events	
Excern autor Support Puttorn Learning Gener Crace Online Puttor Tomo (O Server) & Crace Systems		Total Requests       37/M Total ▲ 10% vn. previ       2500       500       500       500       500       500	n 11pn 4am	Total Blocks 0 Total - Sive previous 24 hours No Results Found Try expanding the time range of your search	Security Blocks 0 Total - % via, previous 24 hours No Results Found Try expanding the time range of your search.	



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

< Back To Multi-org Console				Q, Current Organization: RedIRIS	_
Cisco Umbrella		Select a Delivery Schedu	le		LAST 24 HOLRS *
Overview		We'll regularly email you reports manage the reports we send yo	based on the information below. You can u via your scheduled reports list.	Schedule	
Deployments >	Messages	Daily			
Reporting	Umbrella Open API The new API experience legacy Umbrells APIs yo	9:00 am		ys and select what they can do. There will be no immediate impact to the $~~ imes~~ imes~~ imes~$	
Admin >	Malware: 0 requests block	Report Range			
Selina Garcilopez      RedIRIS	Cryptomining: 0 requess	<ul> <li>Last Calendar Day</li> <li>Last 24 Hours</li> </ul>			
Need Help? 24/7 Phone Support <b>Click Here</b>	Active Networ 9 / 59 Active	Weekly O Monthly		Cos Active Virtual Appliances 0 / 0 Active	
Service Status <ul> <li>All services are operational</li> </ul>	Network Breakdow	CANCEL	BACK CONTINUE	See All Security Events	
Documentation Support Pletform Learning Center Cisco Orkine Pinacy Statement	Total Requests 3.7/M Total _ 16% vs 250K	previous 24 hours	Total Blocks O Total = % vs. previous 24 hours	Security Blocks 0 Total = % vs. previous 24 hours	
© Cace Systems	Signation ton	for 11pm 4am	No Results Found Try expanding the time range of your search.	No Results Found Try expanding the time range of your search.	

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

, , , , , , , , , , , , , , , , , , ,		Q Current Organization: RedIRIS	
e dide Overview	Choose recipients		LAST 24 HOURS 🔻
	manage the reports we send you via your scheduled reports list.		
	Report Title		
Messages	New Overview Scheduled Report		
Umbrella Open APIs at The new API experience ma	Email	is and select what they can do. There will be no immediate impact to the	
legacy Umbrella APIs you a Maharar: 0 rad vasts blocked	Separate multiple emails with a comma or semicolon.		
Botnet: 0 requests blocked in			
Cryptomining: 0 requests bio			
Deployment Health (15%) <b>9</b> / 59 Active Network Breakdown		Active Virtual Appliances 0 / 0 Active	
Total Requests 3.7M Total 🛦 16% vs. pr	Total Blocks vious 24 hours 0 Total = % vs. previous 24 hours	Security Blocks 0 Total - % vs. previous 24 hours	
2555 358 	No Results Found Try expanding the time range of your search.	No Results Found Try expanding the time range of your search.	



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

< Back To Multi-org Console						Q Current Organization: RedIRIS	X
Cisco Umbrella <sup>Overview</sup>	Cisco.	Reporting / Management Scheduled Reports					Schedule
Deplayments >							
Policies >	Q, Search b	by report name, type, frequency, or recipien	t.				
Reporting ~	Marrie		Bernet Trees	F	Basisian	Hara Dallaran	
Core Reports	Name 🗸		Report Type	rrequency	respens	NEXT DEIVERY	
Security Activity	Reporte B	loqueos en Rediris	Security Overview	Daily	selina.garcilopez@externos.rediris.es	sep. 2, 2022 9:30 AM	2
Activity Search							1-1of1 < >
App Discovery							
Top Threats							
Additional Reports							
Total Requests							
Activity Volume							
Top Destinations							
Top Categories							
Top Identities							
Management							
Exported Reports							
Scheduled Reports							
Admin Audit Log							
Investigate >							

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

Come Costada Ayeda Iana Maldo Pulencia Ayeda Gogan 0
Const. Aregonder: Aregonder: Ander Ander Gan. Mr. 4- Acconst.
The first constants of the second of the sec
aluman , cisco
Daily Security Report
In the last day, we've seen:
Automatic a station day
O common a common a common a common a comm
O President STOLESTS
Top Security Events or convex
Connain Requests Identifies The delete for the general
NY KIENITY Vonde
Internal Antonio Anton
Application Discovery and Control (Data from the last 90 days)
5.56K teocoratio and area 162 162 teocoratio and area 162 teocoratio and area 162 teocoratio 162 162 162 162 162 162 162 163 163 163 163 163 163 163 163
CONTROLLED CLOUD APPS SEEALL> SEEALSE
Deployment Summary NETWORKS HEARING CLENTS VIRTUAL AVYLANCES
SCH N TOURBRELLA
Edit Report   Unsuboritie

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:

< Back To Multi-org Console	Q, Current Organization ResBR5
Cisco Umbrella	
Overview	
Deployments >	Set in sonie son-on us SAM. for [Initials distributed lasts and new's on the status of foun-step and/steps for usur promot
Policies >	
Reporting >	
Investigate >	SAML Dashboard User Configuration
Admin $\checkmark$	
Accounts	Clicc Untrivial supports Security Assertion Markup Language or SAML for loging to the Untrivial databated. This allows you to provide single sign-on (SSSO) access to Untrivial ausing enterprise identity providers such as one of the University of the University and the University of the University
User Roles	Status   Disabled
Log Management	Provider None
Authentication	ENGLESAD
Bypass Users	
Bypass Codes	Two-Step Verification
API Keys	This indicates whether two-stee verification (2FA) is enabled for your user account. If you wish to enable this feature, newsate to Admin > Accounts and excand the account work loaded in as by clicking on the account
Licensing	Iname, then select Enable to get started. For more information, see Unitrelia's Heip.
Selina Garcilopez >     RedIRIS	Status   Enabled
Need Hein?	
24/7 Phone Support Click Here Service Status	

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

< Back To Multi-org Console	Q, Current Organization: RedIRIS
Cisco Umbrella	e duthentication
Overview	
Deployments >	East us plante size, as US EAN. for Laboratio doubleased users and about an two ratios of two ratios and users from unification for users and
Policies >	de op singe sy roin is own to oninelle desidele des sind clear to i sie send or mo-sep reincedel no jou account.
Reporting >	
Investigate >	SAML Dashboard User Configuration
Admin 🗸 🗸	
Accounts	Step 1 of 3
User Roles	Select Umbrella SAML Provider
Log Management	Select the SAML provider you'd like to authenticate users to Umbrelia.
Authentication	Cisco SecureX sign-on
Bypass Users	O Prigit
Bypass Codes	
ADI Kene	
Normal Sec.	O Other
Licensing	CANCEL NEXT
Selina Garcilopez > RedIRIS	
Need Help?	Two-Step Verification
24/7 Phone Support Click Here Service Status All services are operational	This indicates whether two-step verification (2FA) is enabled for your user account. If you wish to enable this feature, navigate to Admin > Accounts and expand the account you're logged in as by clicking on the account name, then select Enable to get started. For more information, see Unbriella's Help. Status • Phatiwed



• 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.

< Back To Multi-org Console	Q. Currete Organization: RedRIS
Cisco Umbrella	
Overview	Step 3 or 4 Upload and Verify Other Metadata
Deployments >	Configure University to your SAML provider by selecting one of the following two options: uploading the XML metadata file or filling out required fields for your SSO manually. For more information on how to
Policies >	do this, please see our SAML setup guides.
Reporting >	Select a method
Investigate >	O Menual Configuration
Admin 🗸	XML File Upload
Accounts	
User Roles	
Log Management	Drag and Drag File Here
Authentication	Criselect file
Bypass Users	
Bypass Codes	CANCEL PREVIOUS REXT
API Keys	
Licensing	Two-Step Verification
Selina Garcilopez >     RedIRIS	This indicates whether two-step verification (2FA) is enabled for your user account. If you wish to enable this feature, navigate to Admin > Accounts and expand the account you're logged in as by clicking on the account name, then select Evable to get started. For more information, see Umorelia's Help.
Need Help?	Status 🔮 Enabled
24/7 Phone Support Click Here	

#### 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



Cisco Umbrella		Add a new network Start by pointing your network's DNS to our servers:	۲
Verview		IPv4: 208.67.220.220 and 208.67.222.222	Add
Deployments	A population may be a single public ID address (sta	IPv6: 2620:119:35::35 and 2620:119:53::53	Add a patient's to limited to actual protection to an device that concerts to the interest from
Core Identities	behind that network's IP space. The public IP of y	lo ne	and a network to oniciera to extend protection to any device that connects to the internet non
Networks		Network Name	
Network Devices	Q. Search with a network name or IP adv		
Rearning Computers		IPv4 only     IPv6 only     Mixed IPv4 & IPv1	8
Mobile Devices	Name 🛦	IPv4 Address	Status
Chromebook Users	Acceso Alcatel/Telefónica	0.0.0.0 / Select V	Inactive
Users and Groups		This network has a dynamic IP address. Learn More >	
Configuration	Acceso gestión Geant	CANCEL SAVE	Inactive
Domain Management	Acceso gestor canalink		Inactive
Sites and Active Directory	Annual and CADA		a heating
Internal Networks	ACCESO TEU SARA	130.206.160.0/29 Default Policy	U macuve
Root Certificate	Acuntia Acceso servicio remoto operación re	ed 130.206.192.160/27 Default Policy	Inactive
Service Account Exceptions	Balanceadores	2001:720:418:cafd::/64 Default Policy	Inactive
olicies	CRUE-TIC	130.206.192.80/29 Default Policy	Inactive
leporting	>		
westigate	DMZ	130.206.2.192/28 Default Policy	Inactive
ldmin	Eduroam, TMPEVENT	130.206.16.0/24 Default Policy	inactive
Selina Garcilopez	Caption EM/ADE		A Inactive

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:

< Back To Multi-org Console	Q Currer Organization: Restitis			
Cisco I Imbrella				
	Step 3 of 4			
Overview	Lalaad and Verify Other Metadata			
Deployments >	configure Unitaria to work with your SAML provider to selection one of the following two options: unloading the XML metadata file or filing our required fields for your SSO manually. For more information on how to			
Policies >	do this, please see cur SAML setup guides.			
Reporting >	Select a method			
Investigate >	Manual Configuration			
Δdmin √	O XML File Upload			
	Entity ID			
Accounts	https://rest.my.company.com			
User Roles	Sign On URL			
Log Management	https://test.my.com/adp/endpont/HttpR			
Authentication	Logout URL			
Bypass Users	https://test.my.com/adfs/is/IDPLogout			
Runase Codes	X509 Certificate			
	Encoded Certificate			
API N898				
Licensing				
🕥 Selina Garcilopez 🛛 🚿				
RedIRIS				
	CANCEL PREVOUS NEXT			
Need Help? 24/2 Phone Support				
Click Here				
Service Status	Two-Step Verification			
<ul> <li>All services are operational</li> </ul>				

## 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 <u>dnsfirewall@rediris.es</u>

#### ¿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.

< Back To Multi-org Console		Q Current Organization: RedIRIS	~
Cisco Umbrella	e cisco. Reporting / Care Reports Activity Search	B thesia Epport CSV	HOURS ¥
Deployments >			
Policies >	FILTERS Q. Search by domain, ide	ntty, or URL Advanced - 🗃 Customize C	Columns
Reporting $\checkmark$			
Core Reports	Q. Search filters	2.568.473 Total O Viewing activity from sep. 1, 2022 8:37 AM to sep. 2, 2022 8:37 AM Results per page: 50 💌 1 - 50	$\langle \rangle$
Security Activity	Response Select All	Identity Policy or Ruleset Identity I Destination Inten	nal IF 🗲 🖂
Activity Search	Allowed	🚠 Resolver ofelia rediris es BIND 🚓 Resolver ofelia rediris es BIND artisticcopy.com	
App Discovery	Selectively Proxied	n Resolver ofelia rediris.es BIND n Resolver ofelia rediris.es BIND a57.sosvox.org	
Top Threats		🚠 Resolver ofelia rediris es BIND 🛛 🚠 Resolver ofelia rediris es BIND ns12. bsnl. in	
Additional Reports	Event Type Select All	📅 Resolver bacterio rediris es BIND 👘 Resolver bacterio rediris es BIND outlook.ha.office365.com	
Total Requests	Destination List	📅 Resolver ofelia rediris es BIND 🛛 🛱 Resolver ofelia rediris es BIND 🛛 mail-db5eur02on2047.outbound.protection.outlook.com	
Activity Volume		Resolver ofelia.rediris.es BIND     A Resolver ofelia.rediris.es BIND     Iidsen.com	
Top Destinations	Identity Type Select All	🚠 Resolver ofelia rediris es BIND 👘 Resolver ofelia rediris es BINDdmarc.4gclinical.com	
Top Categories	AD Users	m Resolver ofelia rediris.es BIND m Resolver ofelia.rediris.es BIND sendgrid.net	
Too Identities	Roaming Computers	🚠 Resolver ofelia.rediris.es BIND 🛛 🚠 Resolver ofelia.rediris.es BIND xvfmfzv.outbound-mail.sendgrid.net	
Management	A Networks	📩 Resolver ofelia.rediris.es BIND 📅 Resolver ofelia.rediris.es BIND spbu.ru	
	Sites	🚠 Resolver ofelia.rediris.es BIND 🛛 🚠 Resolver ofelia.rediris.es BIND spf.informaniak.ch	
Exported Reports	O Chromebook Users	📩 Resolver bacterio rediris.es BIND 🕺 Resolver bacterio rediris.es BIND atm-settingsfe-prod-geo2.trafficmanager.net	
Scheduled Reports	· · · ·	🚠 Resolver bacterio rediris es BIND 🔹 Resolver bacterio rediris es BIND settings-prod-weu-2.westeurope.cloudapp.azure.com	
Admin Audit Log	Security Categories Select All	📩 Resolver ofelia rediris es BIND 👘 Resolver ofelia rediris es BIND mta-70-35-113.ikea.com sparkpostmail.com	
Investigate >	Command and Control	🚠 Resolver ofelia rediris es BIND 👘 Resolver ofelia rediris es BIND steinbeis-europa de	

### ¿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-