Comunidad de Cisco

Community Live event

Umbrella Roaming Client-Diagnóstico de fallas

Luis Silva, Ingeniero de Soporte Técnico, CISSP, CCIE #36825

Eduardo Salazar, Sr. Service Delivery Manager

Diciembre 18, 2019

Novedades & Eventos próximos

Ask Me Anything– Sesión del evento

Hasta el Viernes 20 Diciembre, 2019

Con
Luis Silva & Eduardo Salazar

http://bit.ly/ama-umbrella-dec19

Luis Silva
Ingeniero de Soporte Técnico
CCIE #36825

Eduardo Salazar
Sr. Service Delivery Manager

Evento Ask Me Anything – ¡El último del año!

Configuración, Implementación y Troubleshooting de Redes Wireless AirOS

Hasta el viernes 20
Diciembre 2019

Con
Daniel Ordoñez

Cisco Champion

CISCO DESIGNATED VIP PROGRAM

http://bit.ly/pregunteAirOS

Programa Especial – Community Helping Community

Únase a Cisco para ayudar a Doctors Without Borders *(Médicos Sin Fronteras)* a brindar asistencia médica en donde más se necesita.

Hasta Enero 2019

Conozca más

http://bit.ly/chelpc-slides-es

Califique el contenido de la Comunidad de Cisco en Español

¡Califique “Discusiones, Documentos y Videos!

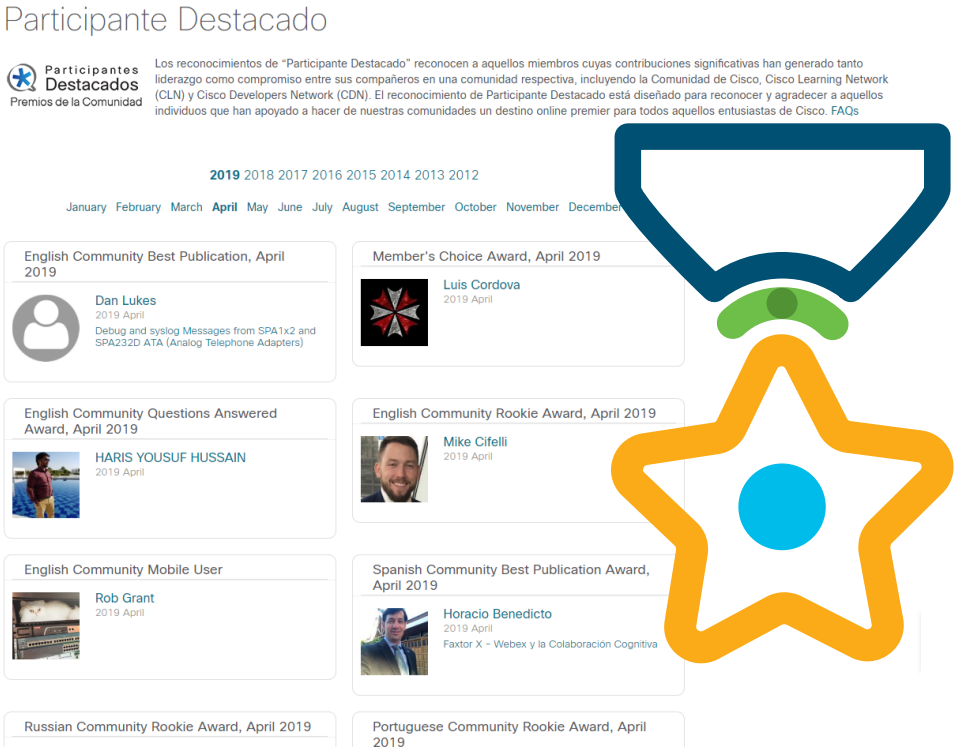
Ayúdenos a identificar el contenido de calidad y a reconocer el esfuerzo de los integrantes de la Comunidad

Reconocimientos en la Comunidad

Participante Destacado

Reconocimiento mensual

Diseñado para reconocer y agradecer a quienes colaboran en la comunidad:
publicando contenido o participando en discusiones



Gracias por su asistencia el día de hoy

La presentación incluirá algunas preguntas a la audiencia.
Le invitamos cordialmente a participar activamente en las preguntas que le haremos durante la sesión

¡Resuelva su dudas y comparta opiniones!

Expertos de la Comunidad de Cisco

Luis silva
Ingeniero de Soporte Técnico
CCIE #36825

Eduardo Salazar
Sr. Service Device Manager

¡Gracias por estar con nosotros hoy día!

http://bit.ly/cl-slides-dec2019

¡Haga sus preguntas al Panel de Expertos!

Use el panel de preguntas y (**P&R / Q&A**) para preguntar a los expertos.

Sus preguntas serán respondidas eventualmente

Cisco Community

Community Live event

Troubleshooting Umbrella

Luis Silva, Ingeniero de Soporte Técnico, CISSP, CCIE #36825

Eduardo Salazar, Sr. Service Delivery Manager

Diciembre 18, 2019

Agenda

- Introducción
- Pre-requisitos de instalación
- Estados del agente
- Estrategias de diagnostico de fallas

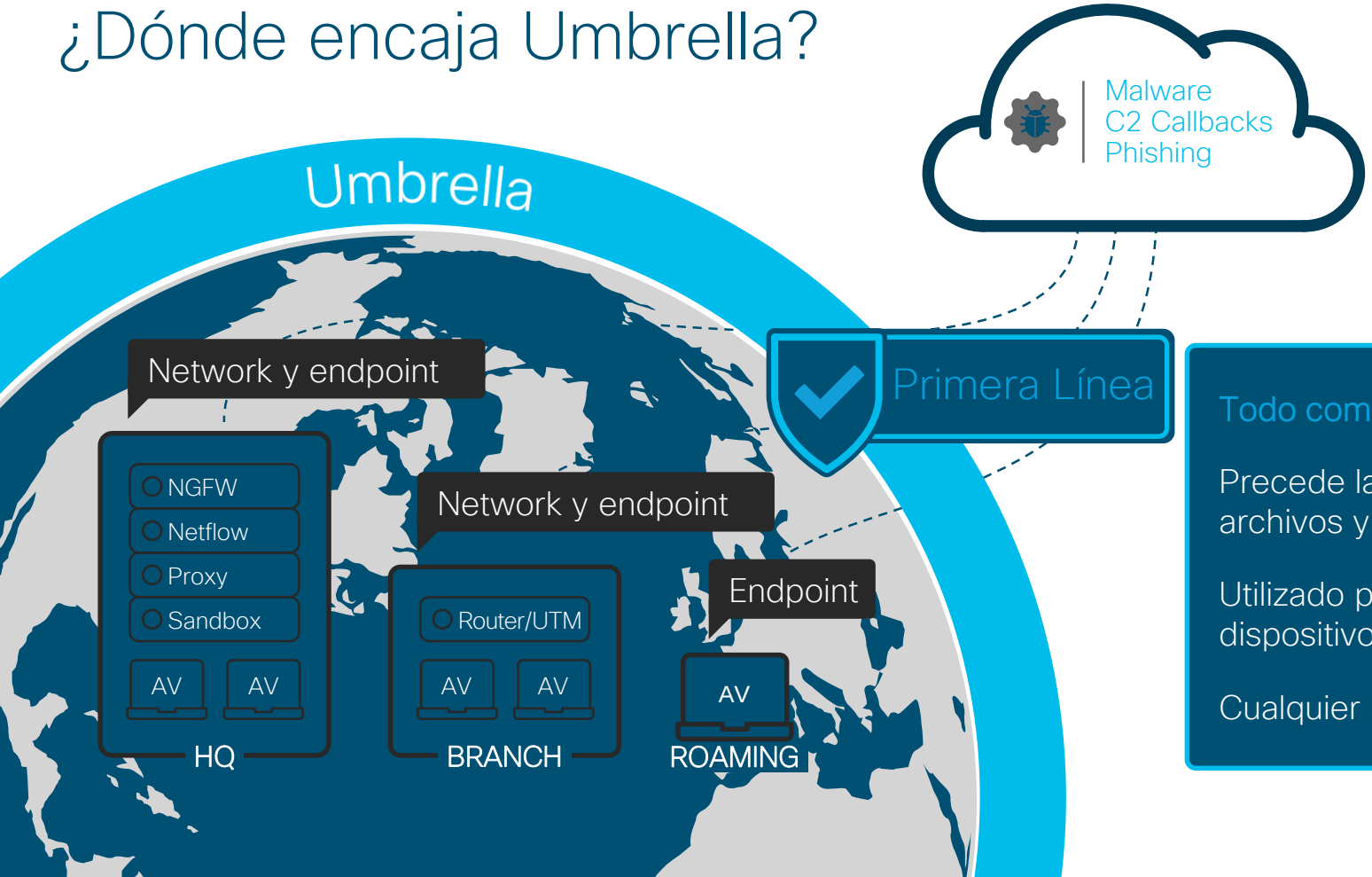
Polling question 1

¿Ha utilizado la solución de seguridad de Cisco Umbrella?

A. Sí

B. No

¿Dónde encaja Umbrella?



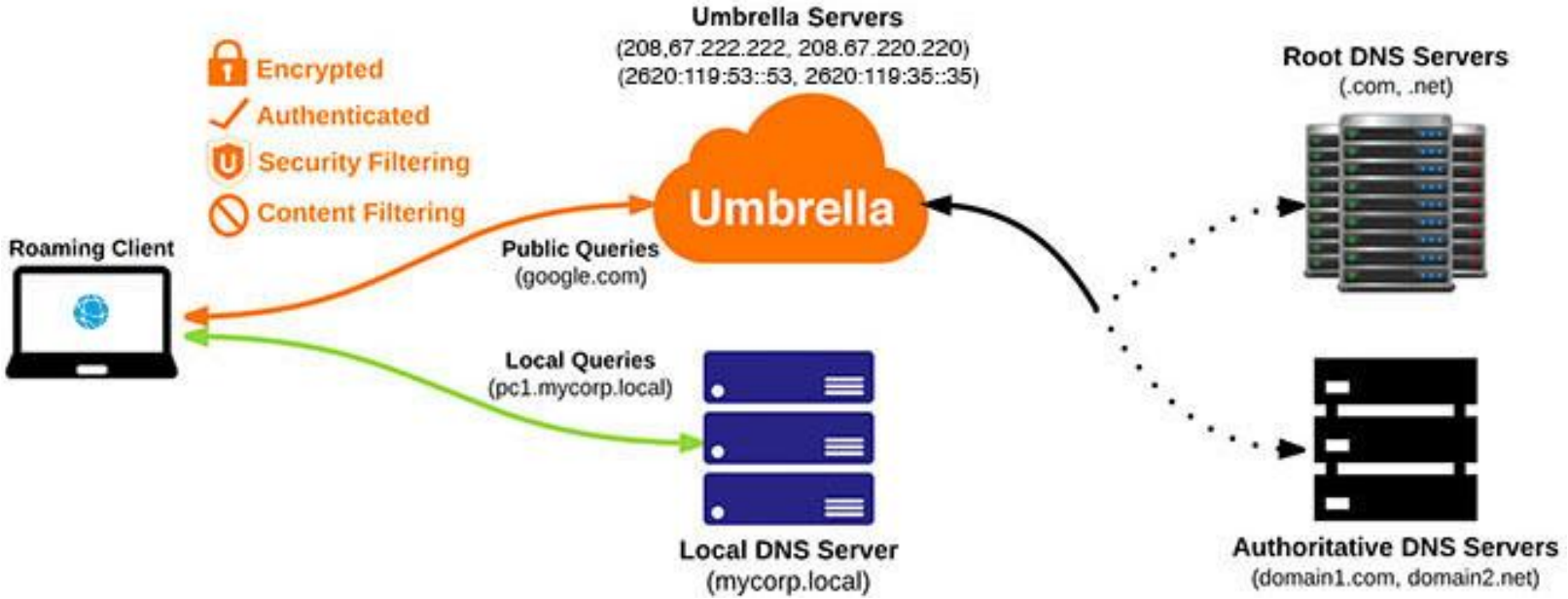
Todo comienza con DNS

Precede la ejecución de archivos y la conexión IP

Utilizado por todos los dispositivos

Cualquier Puerto

Porque el Roaming client



Pre-Requisitos

Pre-Requisitos (ERC)

- Sistemas Operativos Soportados
  - Windows 10 con .NET 4.5
  - Windows 8 (incluye 8.1) (64-bit) con .NET 4.5
  - Windows 7 (64-bit/32-bit) con .NET 3.5.
  - Mac OS X 10.11 o más reciente.

- Sistemas Operativos No Soportados
  - Windows Server (Todas las Versiones)
  - Windows RT (Actualmente no soporta procesadores ARM)
  - Mac OS X 10.8 o anteriores.

Más detalles en: https://docs.umbrella.com/deployment-umbrella/docs/2-prerequisites-update

Pre-Requisitos (AnyConnect)

- Windows 7 (or posterior) x86 (32-bit) and x64 (64-bit)
  - El VPN Module requiere Visual Studio 2015 32-bit runtime.
  - El Roaming Security Module requiere .NET framework (3.5 como mínimo)
- Mac OS X 10.9 (o superior)

- Mínima versión: 4.3 MR1
- Versión mínima recomendada: 4.3 MR4

Pre-Requisitos – DNS

Port	Protocol	Destination
53	UDP	208.67.222.222 / 208.67.220.220 2620:119:53::53 / 2620:119:35::35
53	TCP	208.67.222.222 / 208.67.220.220 2620:119:53::53 / 2620:119:35::35

Pre-Requisitos – Encripcion

Port	Protocol	Destination
443	UDP	208.67.222.222 / 208.67.220.220 2620:119:53::53 / 2620:119:35::3

Pre-Requisitos – HTTP/HTTPS

- Registro Inicial
- Revisión de disponibilidad de una versión actualizada
- Reporte de status
- Actualización de “internal domains”

Port	Protocol	Destination
80	TCP	crl3.digicert.com and crl4.digicert.com
443	TCP	146.112.255.101, 67.215.71.201, 67.215.92.210, 146.112.255.155, sync.hydra.opendns.com, crl3.digicert.com and crl4.digicert.com

Estados del Agente

Estados de Roaming Client

Estado	Color del ícono	Descripción
Reserved	Gris	*Revision del estado de la conecxion.* Redes no activas.
Open	Amarillo	No se puede conectar con 208.67.222.222 por 53/UDP
Protected	Amarillo	DNS64 detectado. Peticiones de DNS de IPv4 e IPv6 estan protegidas
Transparent	No dot	URC es capaz de conectar con 208.67.222.222 en puerto 53/UDP, pero no 443/UDP

Estados de Roaming Client

Estado	Color del Ícono	Descripción
Encrypted	No dot	443/UDP.
Protected Network	No dot	“Deshabilitar detrás de redes protegidas”
Behind Virtual Appliance	No dot	Se detecto un VA en la red
Unprotected	Rojo	Agente no protegiendo la red

Estados de AnyConnect

Estado	Color del Ícono	Descripción
Reserved	Naranjo	*Revision del estado de la conecxion.* Redes no activas.
Open	Amarillo	No se puede conectar con 208.67.222.222 por 53/UDP
Protected	Verde	Se puede conectar 208.67.222.222 en Puerto 53/UDP, pero no 443 UDP
Encrypted	Verde	Se puede conectar 208.67.222.222 en Puerto 443 UDP

Estados de AnyConnect

Estado	Color del Ícono	Descripción
Protected Network	Verde	“Deshabilitar detrás de redes protegidas”
Behind Virtual Appliance	Verde	Se encuentra un VA en la red
VPN Trusted Network State	Gris	*Red protegida*
Disabled due to VPN State	Gris	*VPN activo*

Estados de AnyConnect

Estado	Color del Ícono	Descripción
No OrgInfo.json State	Rojo	*No hay un perfil*
Agent Unavailable State	Rojo	Servicio no activo
Missing .NET Dependency State (Windows only)	Rojo	Microsoft 4.0 NET framework no instalado

Polling question 2

¿En qué escenarios puedo hacer un despliegue del Roaming client en mis computadoras?

A. Cuando necesito saber el usuario del Directorio Activo

B. Cuando tengo usuarios remotos o fuera de la red

C. Cuando necesito un VPN conectado a todo momento

Deteccion de Fallas

Conectividad Básica

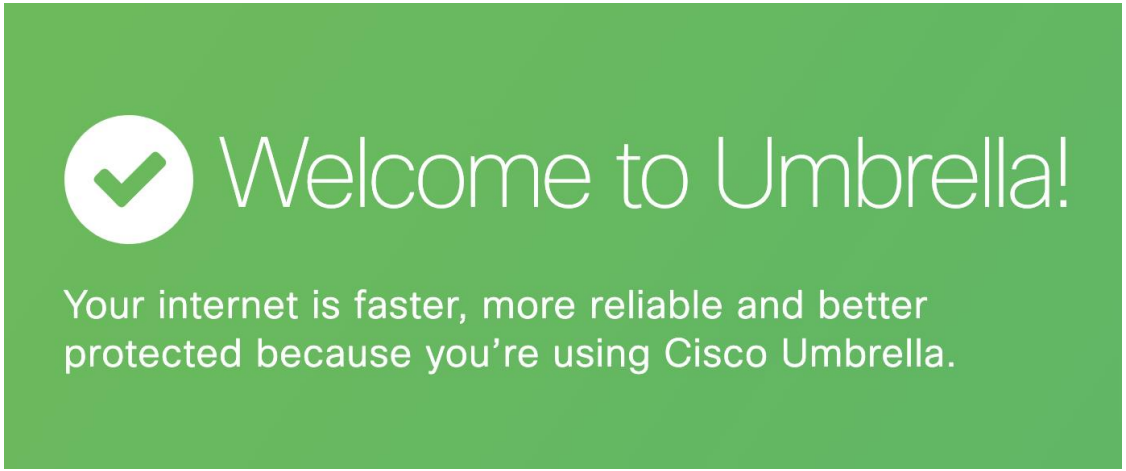
- Wired – Wireless
- IP Address
- Puerta de enlace (DG)
- ARP
- Ping DG
- Ping Internet

Revisar JSON file

- AnyConnect
  - Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\
    o
  - Mac: /opt/cisco/anyconnect/Umbrella/
    Nota: Debe crear la estructura de este folder por adelantado
- Roaming Client
  - C:\ProgramData\OpenDNS\ERC\

Troubleshooting Básico

- Verificación del servicio
  - https://welcome.umbrella.com/



Troubleshooting Básico – Process (/bin/ps wwaux)

/opt/cisco/anyconnect/bin/dnscrypt-proxy --user nobody --local-address=127.0.0.1:53 --plugin=/opt/cisco/anyconnect/lib/libdcplugin_erc.so -d

/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app/Contents/MacOS/Cisco AnyConnect Secure Mobility Client -psn_0_139298

/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app

/opt/cisco/anyconnect/bin/acumbrellaagent -console

Troubleshooting Básico – Process (Windows)

- AnyConnect:
  - acumbrellaagent.exe
- Standalone:
  - ERCService.exe

Folders Importantes (Roaming Client)

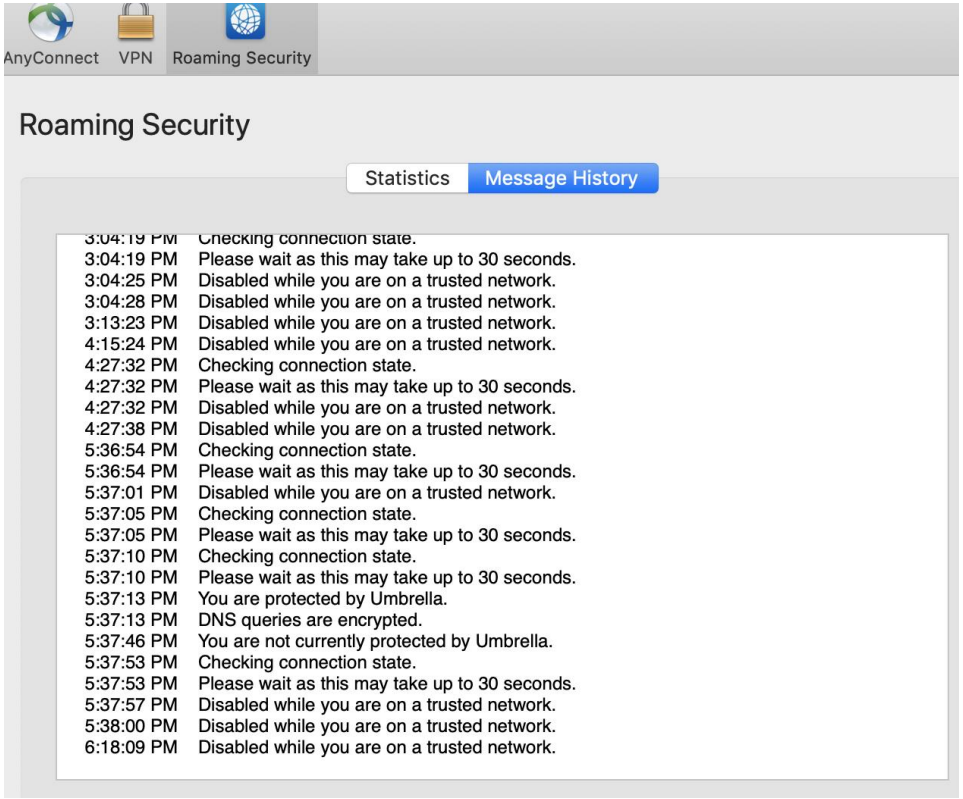
- Logs
  - C:\ProgramData\OpenDNS\ERC\Open DNS_ERC_Service.log
  - C:\ProgramData\OpenDNS\ERC\OpenDNS_ERC_UI.log
- Otros Archivos
  - C:\Program Files (x86)\OpenDNS\OpenDNS Enterprise Roaming Client – The default install path.
  - C:\ProgramData\OpenDNS\ERC\manifest.json – Indicates what version to upgrade to, if not matching.
  - C:\ProgramData\OpenDNS\ERC\OrgInfo.json – Contains organizationId, fingerprint, and userId.

Folders Importantes (Roaming Client)

- C:\ProgramData\OpenDNS\ERC\resolv.conf – Almacena IPs de los servidores originales DNS para requisiciones proxying NXDOMAIN DNS (ejemplo: para buscar recursos LAN).
- C:\ProgramData\OpenDNS\ERC\whitelist – Permite la Lista de Dominio(s) [desde Dominios internos (Roaming) en el dashboard]; whitelist.txt es removido si los dominios no son colocados.
- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\OpenDNS Roaming Client – Comienza el shortcut link para ERCInterface.exe.
- C:\ProgramData\OpenDNS\ERC\Upgrades – La carpeta contiene los instaladores de actualización.
- C:\ProgramData\OpenDNS\ERC\Dumps\OpenDNSService_MM_DD_YYYY.mdmp – Si ERC falla, un Dumps dir es creado para almacenar dump files.

AnyConnect Estadísticas

AnyConnect Estadísticas



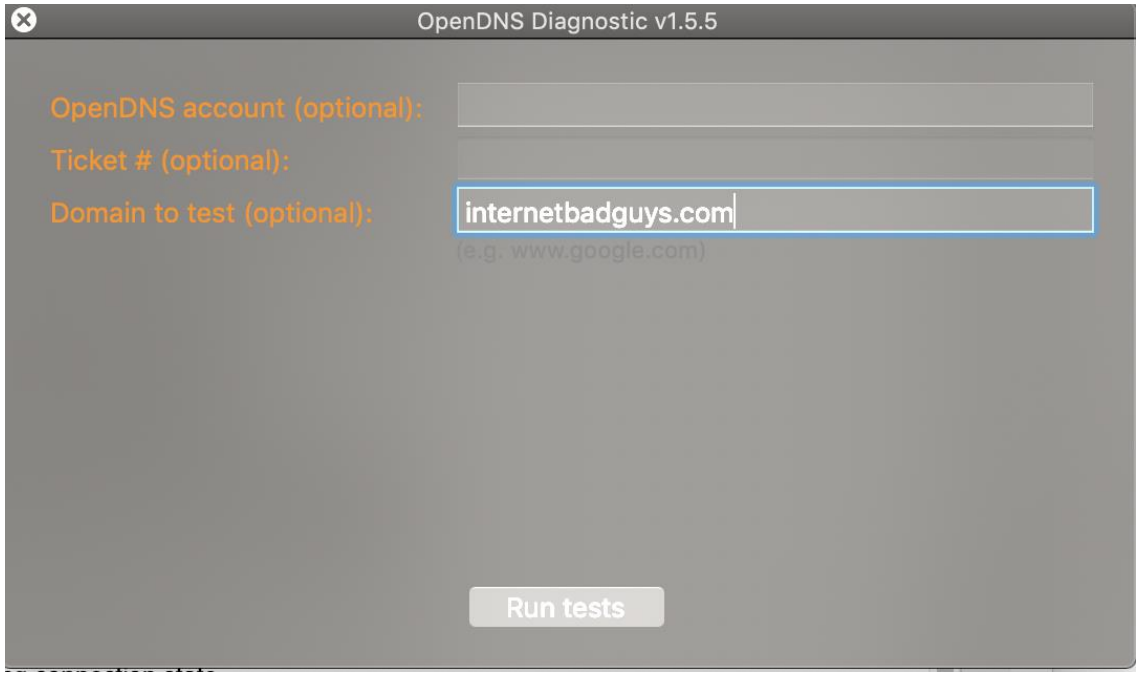
Diagnósticos (Diagnostics)

- Windows:
  %Program Files (x86)%\Cisco\Cisco AnyConnect Secure Mobility Client\UmbrellaDiagnostic.exe
- Mac OS X:
  /opt/cisco/anyconnect/bin/UmbrellaDiagnostic.app/

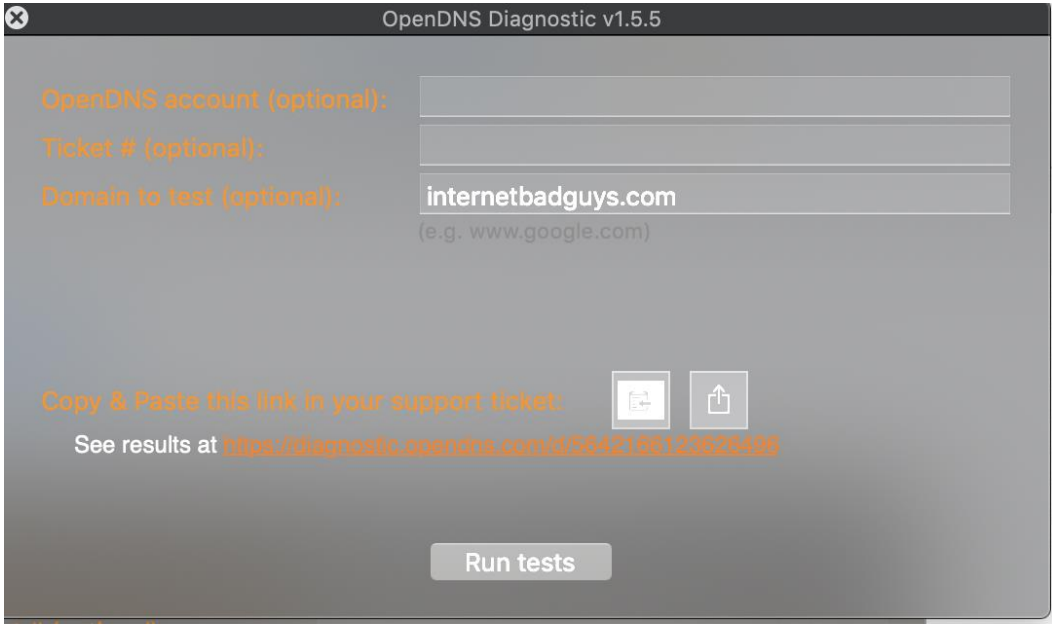
- Descargar “Diagnostic tool”:

https://support.umbrella.com/hc/en-us/articles/234692027-Umbrella-Diagnostic-Tool

Diagnostics



Diagnostics



Troubleshooting Básico – Mi IP address

```
Results for: /usr/bin/dig +time=10 myip.opendns.com
stdout:

; <<>> DiG 9.10.6 <<>> +time=10 myip.opendns.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52022
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;myip.opendns.com.              IN      A

;; ANSWER SECTION:
myip.opendns.com.       0       IN      A       152.231.169.37

;; Query time: 87 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Wed Aug 14 06:40:21 CST 2019
;; MSG SIZE  rcvd: 66
```

Windows command: nslookup myip.opendns.com

Troubleshooting Básico – Dig

```
Results for: /usr/bin/dig +time=10 internetbadguys.com
stdout:

; <<>> DiG 9.10.6 <<>> +time=10 internetbadguys.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59615
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;internetbadguys.com.           IN      A

;; ANSWER SECTION:
internetbadguys.com.    0       IN      A       146.112.61.108

;; Query time: 153 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Wed Aug 14 06:40:22 CST 2019
;; MSG SIZE  rcvd: 72
```

Windows command: nslookup internetbadguys.com

Troubleshooting Básico– Dig 208.67.222.222

```
Results for: /usr/bin/dig +time=10 internetbadguys.com @208.67.222.222
stdout:

; <<>> DiG 9.10.6 <<>> +time=10 internetbadguys.com @208.67.222.222
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63823
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;internetbadguys.com.           IN      A

;; ANSWER SECTION:
internetbadguys.com.    0       IN      A       146.112.61.108

;; Query time: 184 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Wed Aug 14 06:40:22 CST 2019
;; MSG SIZE  rcvd: 72
```

Windows command: nslookup internetbadguys.com 208.67.222.222

Troubleshooting Basico– Dig 4.2.2.1

```
Results for: /usr/bin/dig +time=10 internetbadguys.com @4.2.2.1
stdout:

; <<>> DiG 9.10.6 <<>> +time=10 internetbadguys.com @4.2.2.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60345
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 8192
;; QUESTION SECTION:
;internetbadguys.com.           IN      A

;; ANSWER SECTION:
internetbadguys.com.    1       IN      A       67.215.92.210

;; Query time: 281 msec
;; SERVER: 4.2.2.1#53(4.2.2.1)
;; WHEN: Wed Aug 14 06:40:22 CST 2019
;; MSG SIZE  rcvd: 64
```

Windows command: nslookup internetbadguys.com 4.2.2.1

Umbrella Block Page – Direcciones IPs

Name	Record Type	Address
Domain List Block Page	a	146.112.61.104
Domain List Block Page	aaaa	::ffff:146.112.61.104
Command and Control Callback Block Page	a	146.112.61.105
Command and Control Callback Block Page	aaaa	::ffff:146.112.61.105
Content Category Block Page	a	146.112.61.106
Content Category Block Page	aaaa	::ffff:146.112.61.106
Malware Block Page	a	146.112.61.107
Malware Block Page	aaaa	::ffff:146.112.61.107
Phishing Block Page	a	146.112.61.108
Phishing Block Page	aaaa	::ffff:146.112.61.108
Security Integrations Block Page	a	146.112.61.110
Security Integrations Block Page	aaaa	::ffff:146.112.61.110

Troubleshooting Básico – Traceroute

```
Results for: /usr/sbin/traceroute -I -w 2 internetbadguys.com
stdout:
 1  * 192.168.0.1 (192.168.0.1)  2.319 ms *
 2  * * *
 3  10.48.0.1 (10.48.0.1)  18.306 ms  26.378 ms  12.082 ms
 4  172.16.8.9 (172.16.8.9)  15.090 ms  13.692 ms  14.585 ms
 5  172.16.7.61 (172.16.7.61)  313.562 ms  17.858 ms  15.288 ms
 6  172.16.7.201 (172.16.7.201)  13.328 ms  30.826 ms  13.855 ms
 7  190.242.136.78 (190.242.136.78)  20.178 ms  15.966 ms  12.774 ms
 8  ae15.brx-mx2020-1.boca-raton.fl.usa.cwc.com (69.79.100.50)  77.159 ms  78.859 ms  76.624 ms
 9  63-217-112-145.static.pccwglobal.net (63.217.112.145)  66.879 ms  62.295 ms  66.031 ms
10  * * *
11  * * *
12  4.59.240.138 (4.59.240.138)  65.897 ms  68.481 ms  67.131 ms
13  hit-phish.opendns.com (146.112.61.108)  68.865 ms  62.449 ms  62.588 ms

stderr:
traceroute to internetbadguys.com (146.112.61.108), 64 hops max, 72 byte packets
```

Windows command: tracert internetbadguys.com

Troubleshooting Básico – Traceroute

```
Results for: /usr/sbin/traceroute -I -w 2 208.67.222.222
stdout:
 1  192.168.0.1 (192.168.0.1)  5.722 ms  2.294 ms  1.430 ms
 2  * * *
 3  10.48.0.1 (10.48.0.1)  19.977 ms  15.953 ms  13.874 ms
 4  172.16.8.9 (172.16.8.9)  12.903 ms  14.866 ms  14.140 ms
 5  172.16.7.61 (172.16.7.61)  43.374 ms  14.573 ms  16.047 ms
 6  172.16.7.201 (172.16.7.201)  12.791 ms  14.704 ms  16.719 ms
 7  190.242.136.78 (190.242.136.78)  12.190 ms  15.471 ms  12.222 ms
 8  ae15.brx-mx2020-1.boca-raton.fl.usa.cwc.com (69.79.100.50)  75.595 ms  81.234 ms  80.676 ms
 9  63-217-112-145.static.pccwglobal.net (63.217.112.145)  66.727 ms  63.463 ms  64.211 ms
10  * * *
11  * * *
12  4.59.240.138 (4.59.240.138)  66.308 ms  67.676 ms  66.354 ms
13  resolver1.opendns.com (208.67.222.222)  84.070 ms  74.615 ms  73.788 ms

stderr:
traceroute to 208.67.222.222 (208.67.222.222), 64 hops max, 72 byte packets
```

Windows command: tracert 208.67.222.222

Polling question 3

¿Qué URL se utiliza para saber si estamos utilizando Umbrella en la red?

A. Umbrella.welcome.com
B. Welcome.umbrella.com
C. Signup.umbrela.com
D. Ninguna de las anteriores

Troubleshooting Básico – Traceroute

```
Results for: /usr/sbin/traceroute -I -w 2 api.opendns.com
stdout:
 1  * * 192.168.0.1 (192.168.0.1)  2.201 ms
 2  * * *
 3  10.48.0.1 (10.48.0.1)  18.142 ms  30.789 ms  12.019 ms
 4  172.16.8.9 (172.16.8.9)  12.806 ms  16.872 ms  11.938 ms
 5  172.16.7.61 (172.16.7.61)  307.360 ms  13.519 ms  11.749 ms
 6  172.16.7.201 (172.16.7.201)  18.576 ms  13.888 ms  19.524 ms
 7  190.242.136.78 (190.242.136.78)  14.163 ms  17.922 ms  15.003 ms
 8  ae15.brx-mx2020-1.boca-raton.fl.usa.cwc.com (69.79.100.50)  86.736 ms  84.887 ms  85.255 ms
 9  63-217-112-145.static.pccwglobal.net (63.217.112.145)  70.705 ms  69.245 ms  81.579 ms
10  * * *
11  * * *
12  open-dns-in.ear2.sanjose1.level3.net (4.28.12.198)  173.799 ms  171.148 ms  174.830 ms
13  vlan130.fw5.sjc.opendns.com (67.215.78.6)  175.369 ms  236.894 ms  179.874 ms
14  api.opendns.com (67.215.92.210)  173.798 ms  172.692 ms  184.970 ms

stderr:
traceroute: Warning: api.opendns.com has multiple addresses; using 67.215.92.210
traceroute to api.opendns.com (67.215.92.210), 64 hops max, 72 byte packets
```


Windows command: tracert api.opendns.com

Troubleshooting Básico– debug.opendns.com

```
Results for: /usr/bin/dig +time=10 debug.opendns.com txt
stdout:

; <<>> DiG 9.10.6 <<>> +time=10 debug.opendns.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56079
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;debug.opendns.com.             IN      TXT

;; ANSWER SECTION:
debug.opendns.com.      0       IN      TXT     "server m81.mia"
debug.opendns.com.      0       IN      TXT     "device 0101BB10CC6506B7"
debug.opendns.com.      0       IN      TXT     "flags 40036 0 14040 180000000000000024039FD100000000000000"
debug.opendns.com.      0       IN      TXT     "originid 98413381"
debug.opendns.com.      0       IN      TXT     "orgid 1912899"
debug.opendns.com.      0       IN      TXT     "orgflags A4"
debug.opendns.com.      0       IN      TXT     "actype 0"
debug.opendns.com.      0       IN      TXT     "bundle 622726"
debug.opendns.com.      0       IN      TXT     "source 152.231.169.37:60071"
debug.opendns.com.      0       IN      TXT     "dnscrypt enabled (716D496B684B3766)"

;; Query time: 505 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Wed Aug 14 06:40:22 CST 2019
;; MSG SIZE  rcvd: 555
```


Windows command: nslookup -timeout=10 -type=txt debug.opendns.com

Troubleshooting Básico – Ping

```
Results for: /sbin/ping -c 5 rtr1.mia.opendns.com (miami router)
stdout:
PING rtr1.network.mia1.edc.strln.net (204.194.239.1): 56 data bytes
64 bytes from 204.194.239.1: icmp_seq=0 ttl=51 time=94.918 ms
64 bytes from 204.194.239.1: icmp_seq=1 ttl=51 time=94.416 ms
64 bytes from 204.194.239.1: icmp_seq=2 ttl=51 time=94.374 ms
64 bytes from 204.194.239.1: icmp_seq=3 ttl=51 time=94.651 ms
64 bytes from 204.194.239.1: icmp_seq=4 ttl=51 time=95.509 ms

--- rtr1.network.mia1.edc.strln.net ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 94.374/94.774/95.509/0.416 ms
```

* También compruebe la conectividad a DG, ISP

Windows command: ping rtr1.mia.opendns.com

Troubleshooting Básico– DNS config

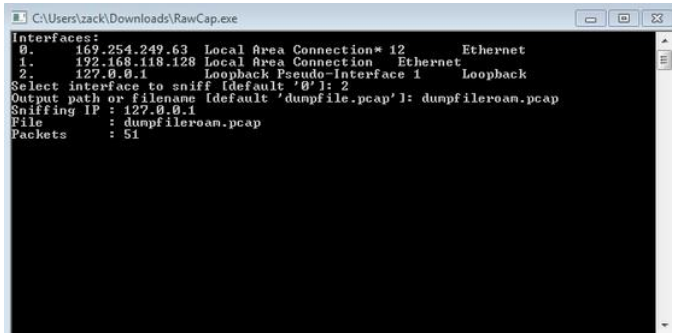
```
Results for: /usr/sbin/scutil --dns
stdout:
DNS configuration

resolver #1
  search domain[0] : Home
  nameserver[0] : 208.67.222.222
  nameserver[1] : 208.67.220.220
  if_index : 8 (en0)
  flags    : Request A records
  reach    : 0x00000002 (Reachable)
```

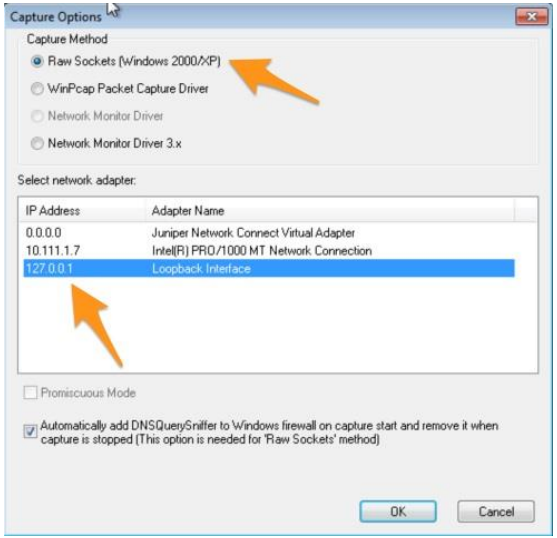
```
Results for: /sbin/ifconfig -a
stdout:
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC0: flags=0<> mtu 0
XHC1: flags=0<> mtu 0
XHC20: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether dc:a9:04:96:9c:e3
        inet6 fe80::c89:814c:ce35:9ddd%en0 prefixlen 64 secured scopeid 0x8
        inet 192.168.0.102 netmask 0xffffff00 broadcast 192.168.0.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

Windows command: ipconfig /all

Troubleshooting Básico- Capturas Windows

- RawCap





- DNSQuerySniffer

https://support.umbrella.com/hc/en-us/articles/230560907-Umbrella-Roaming-Client-Troubleshooting-Packet-and-DNS-Captures

Troubleshooting Básico– Capturas (Ambos)

DNS Only

If you only want to look at DNS requests.

Filter: dns

DNS + HTTP

If you only want to look at DNS and HTTP request.

Filter: dns or http

Filter out debug lookups (probes)

If you are not explicitly testing checking for probe-related issues or issues with debug.opendns.com, you can filter out debug.opendns.com by typing the following in the filter bar:

Filter: dns && not dns contains debug.opendns.com

Troubleshooting Básico – DNS

- https://dnsleaktest.com/results.html

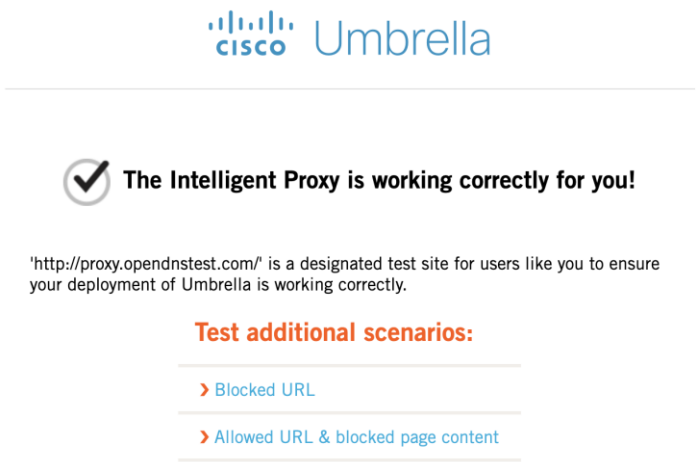
IP	Hostname	ISP	Country
208.69.32.205	pdu3.ash.opendns.com.	Cisco OpenDNS, LLC	Chesapeake, United States
208.69.32.206	pdu4.ash.opendns.com.	Cisco OpenDNS, LLC	Chesapeake, United States
208.69.32.67	m25.ash.opendns.com.	Cisco OpenDNS, LLC	Chesapeake, United States

Información Útil

- Test Phishing:
  - http://www.internetbadguys.com
- Test Malware:
  - http://www.examplemalwaredomain.com
  - http://malware.opendns.com/
- Test CnC:
  - http://www.examplebotnetdomain.com
- Test Content Filtering:
  - http://www.exampleadultsite.com

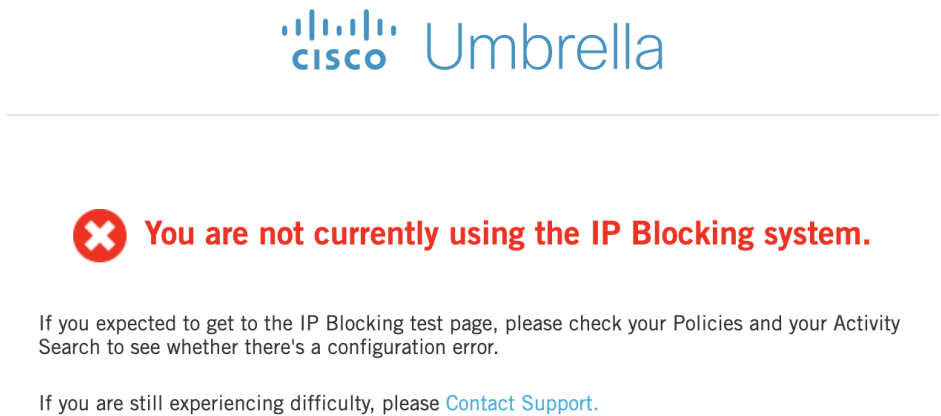
Información Útil

- Intelligent Proxy
  - http://proxy.opendnstest.com/index.html



Información Útil

- IP Layer Enforcement
  - http://ipblock.opendnstest.com/unproxied.html

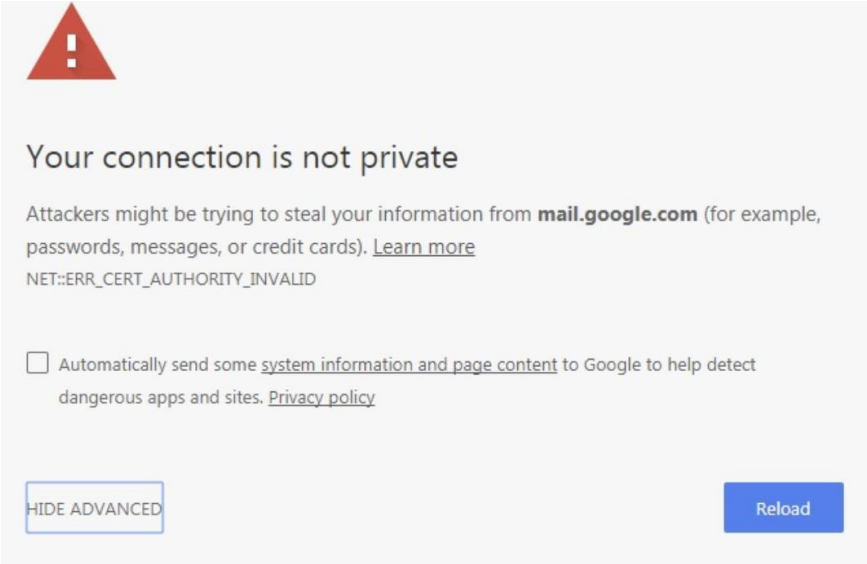


Troubleshooting Básico – Windows

- tracert 208.67.222.222
- tracert 208.67.220.220
- tracert api.opendns.com.
- nslookup -timeout=10 -type=txt debug.opendns.com. 208.67.222.222
- nslookup -timeout=10 -type=txt debug.opendns.com.
- ipconfig /all

Verificar Certificado Cisco

- Para descifrado HTTPS y bloqueo de página, verifique que el certificado de Cisco se encuentre instalado

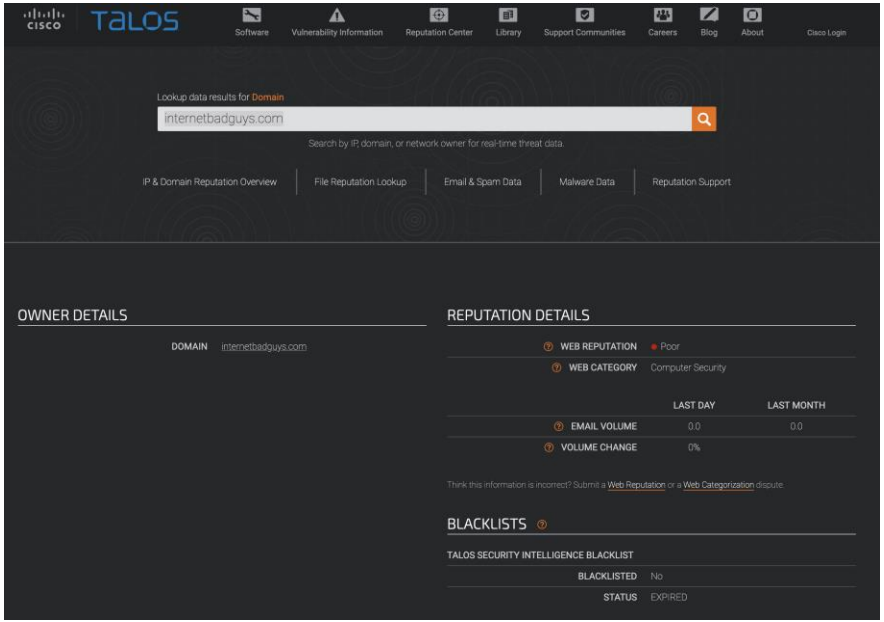


Información Útil

- Compatibilidad VPN
  - https://support.umbrella.com/hc/en-us/articles/230561147-Umbrella-Roaming-Client-VPNs-and-VPN-Compatibility
- Problemas CDN
  - https://support.umbrella.com/hc/en-us/articles/230563447-Akamai-Content-and-Cisco-Umbrella-Understanding-issues-with-CDNs-and-troubleshooting-steps)
- Roaming Client KB
  - https://support.umbrella.com/hc/en-us/sections/206607008-Roaming-Computers-Roaming-Client-

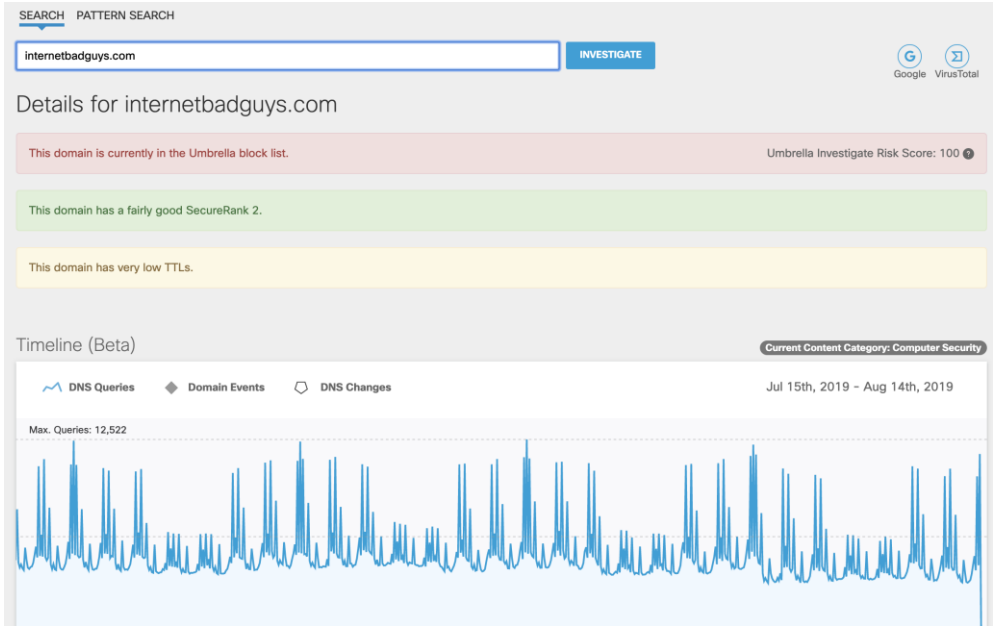
Talos

https://talosintelligence.com/reputation_center/lookup?search=internetbadguys.com



Investigate

https://investigate.umbrella.com/

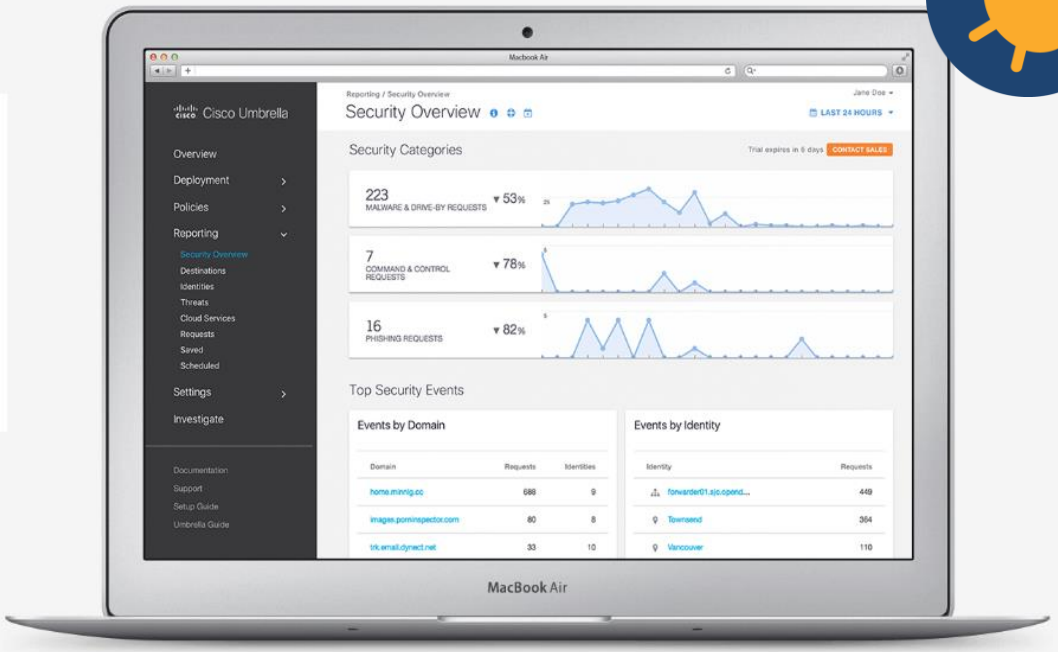


Pruebe Umbrella sin costo

Suscríbase para una prueba gratis

Solo le toma un momento y podrá experimentar los 14 días de prueba de Umbrella

Comience su prueba gratuita



Link: https://signup.umbrella.com/


CISCO

Resuelva sus dudas

Utilice el panel de Q&A o P&R
para realizar sus preguntas

Ask Me Anything– Sesión del evento

Hasta el Viernes 20 Diciembre, 2019

Con
Luis Silva & Eduardo Salazar

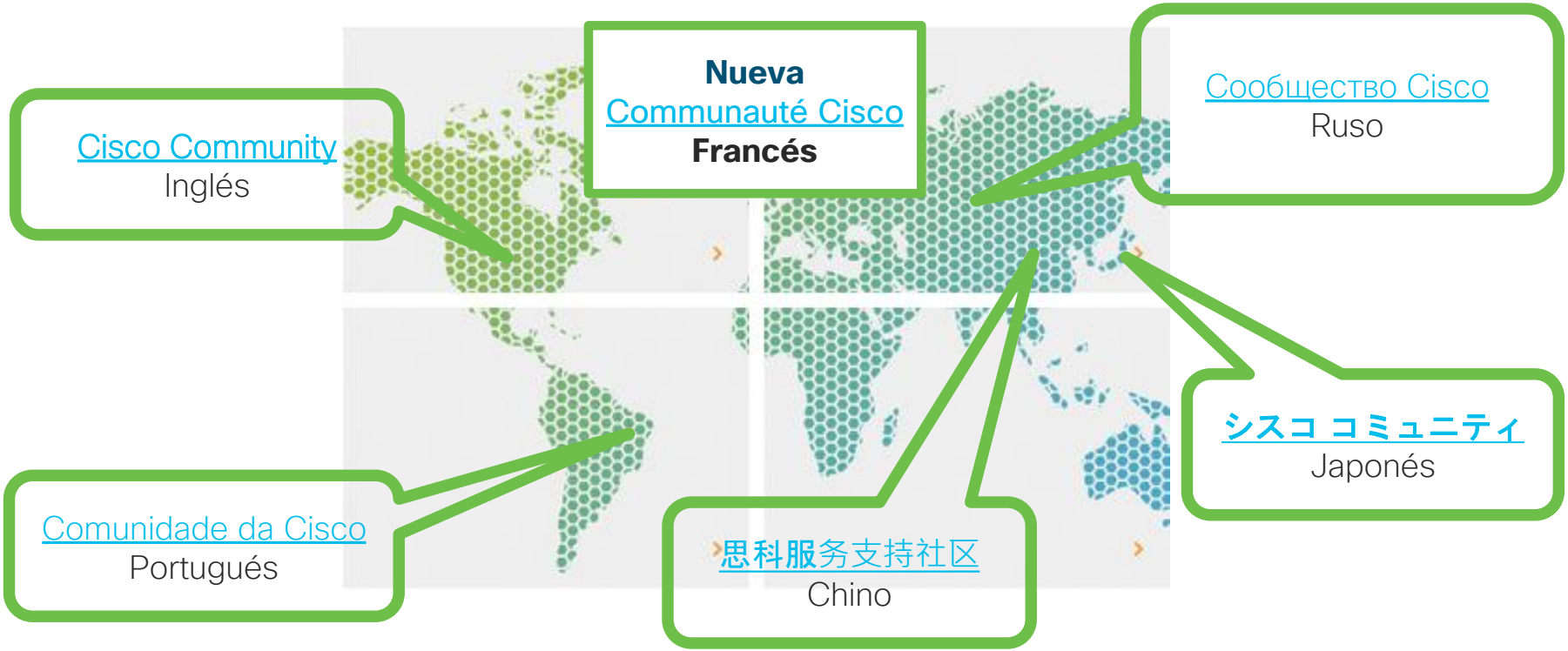
http://bit.ly/ama-umbrella-dec19

Luis Silva
Ingeniero de Soporte Técnico
CCIE #36825

Eduardo Salazar
Sr. Service Delivery Manager

La Comunidad de soporte tiene otros Idiomas

Si habla Portugués, Japonés, Ruso, Chino o Inglés lo invitamos a participar en otro idioma.



Lo invitamos a nuestros próximos eventos en Redes Sociales

Twitter

- @CiscoTSLatam
- @cisco_spain
- @cisco_support
- @Cisco_LA

Facebook

- Cisco TS- Latam
- Cisco España
- Cisco Latinoamérica
- CiscoCommunity

Lo invitamos a nuestros próximos eventos en Redes Sociales

YouTube

- CiscoLatam
- ciscocommunity

App

- Cisco Technical Support

LinkedIn

- Cisco Community

¡Nos interesa su opinión!

Por favor complete la encuesta,
aparecerá en la pantalla de su buscador

¡Gracias por acompañarnos en el último evento del año!


CISCO