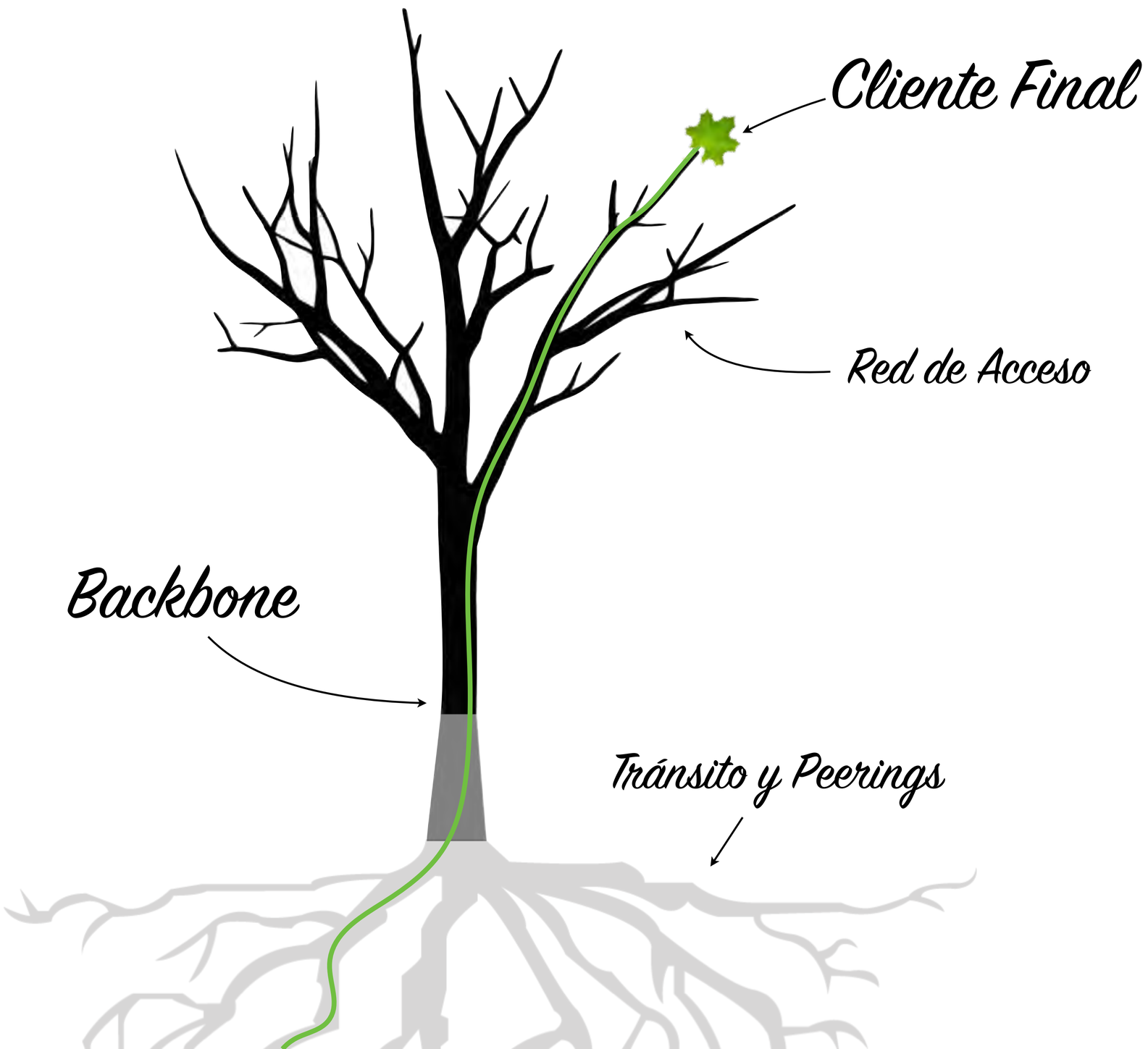
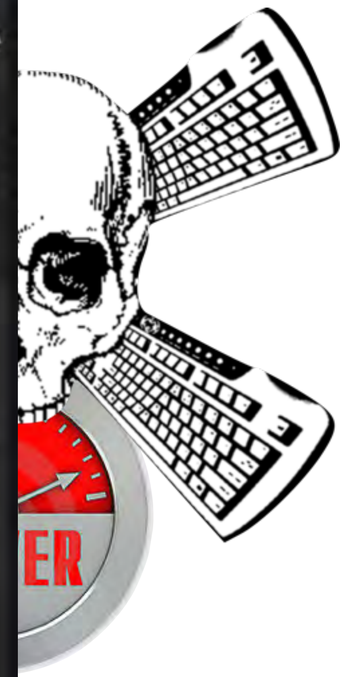
Defensa Perimetral

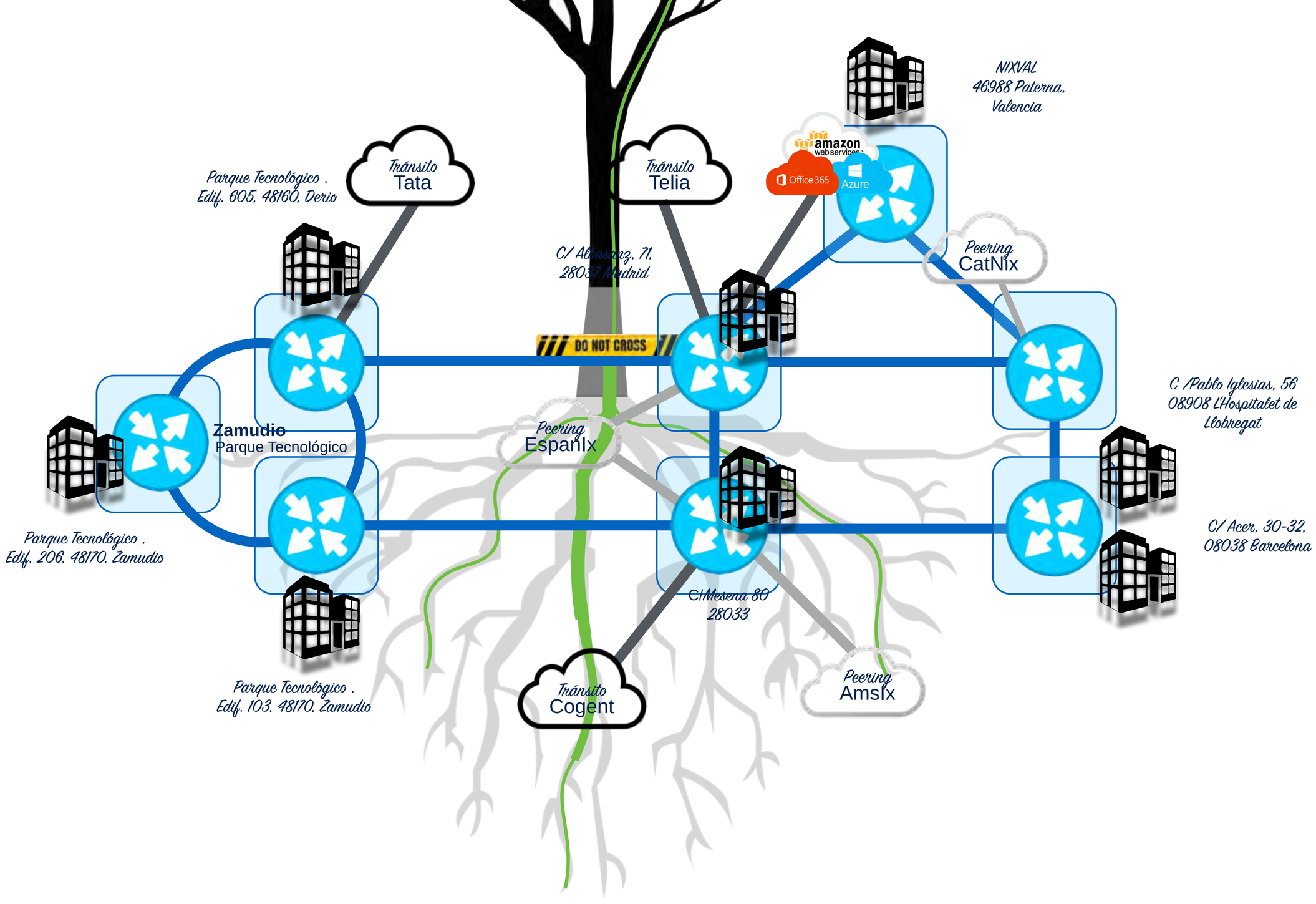

Cliente Final
Red de Acceso
Backbone
Tránsito y Peerings

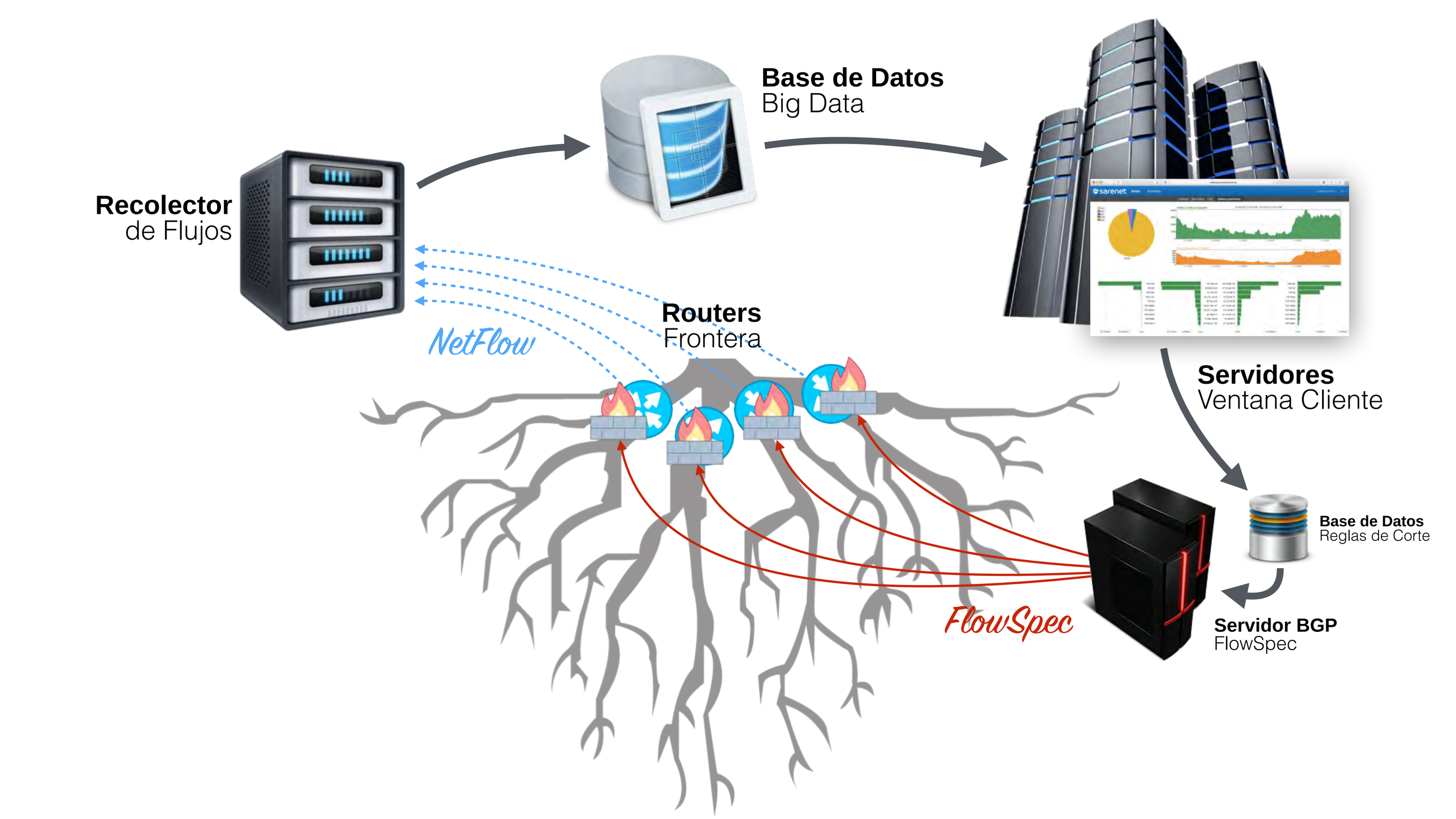

Punto más débil
DO NOT CROSS

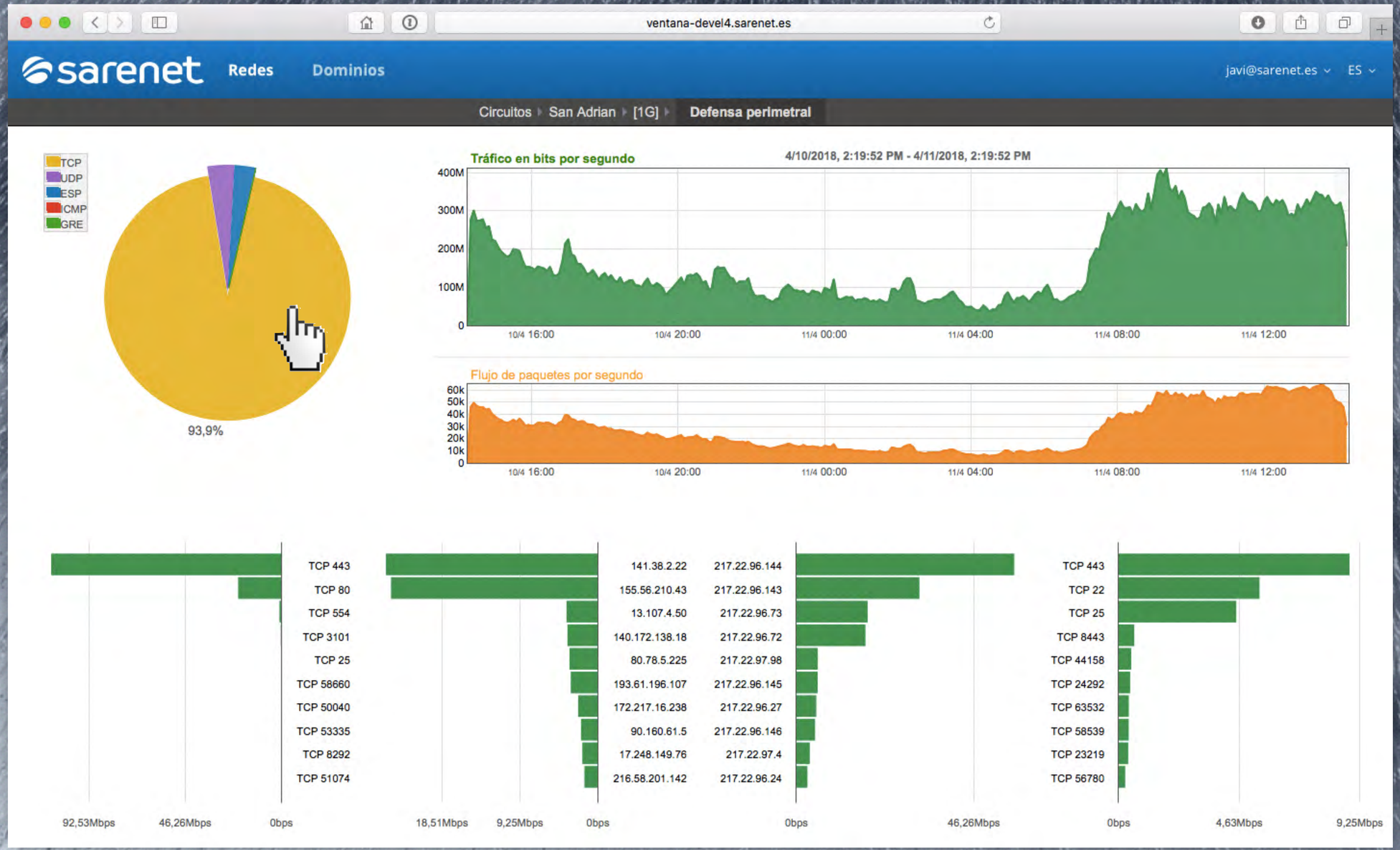
Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent +	**1** Concurrent +	**1** Concurrent +	**1** Concurrent +	**1** Concurrent +
300 seconds boot time	**600** seconds boot time	**1200** seconds boot time	**1800** seconds boot time	**3600** seconds boot time
125Gbps total network capacity	**125Gbps** total network capacity	**125Gbps** total network capacity	**125Gbps** total network capacity	**125Gbps** total network capacity
Resolvers & Tools	**Resolvers** & Tools	**Resolvers** & Tools	**Resolvers** & Tools	**Resolvers** & Tools
24/7 Dedicated Support	**24/7** Dedicated Support	**24/7** Dedicated Support	**24/7** Dedicated Support	**24/7** Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now

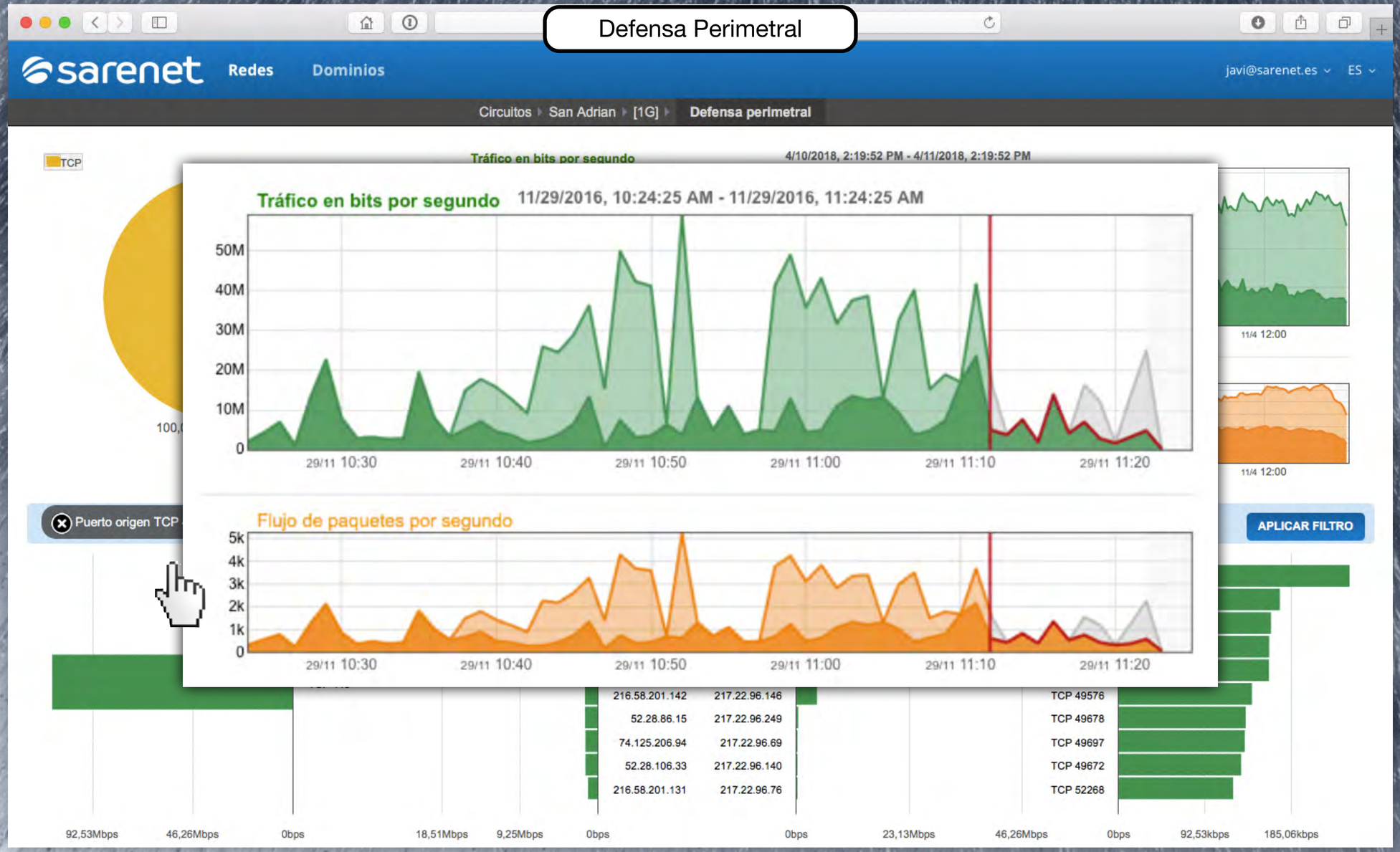


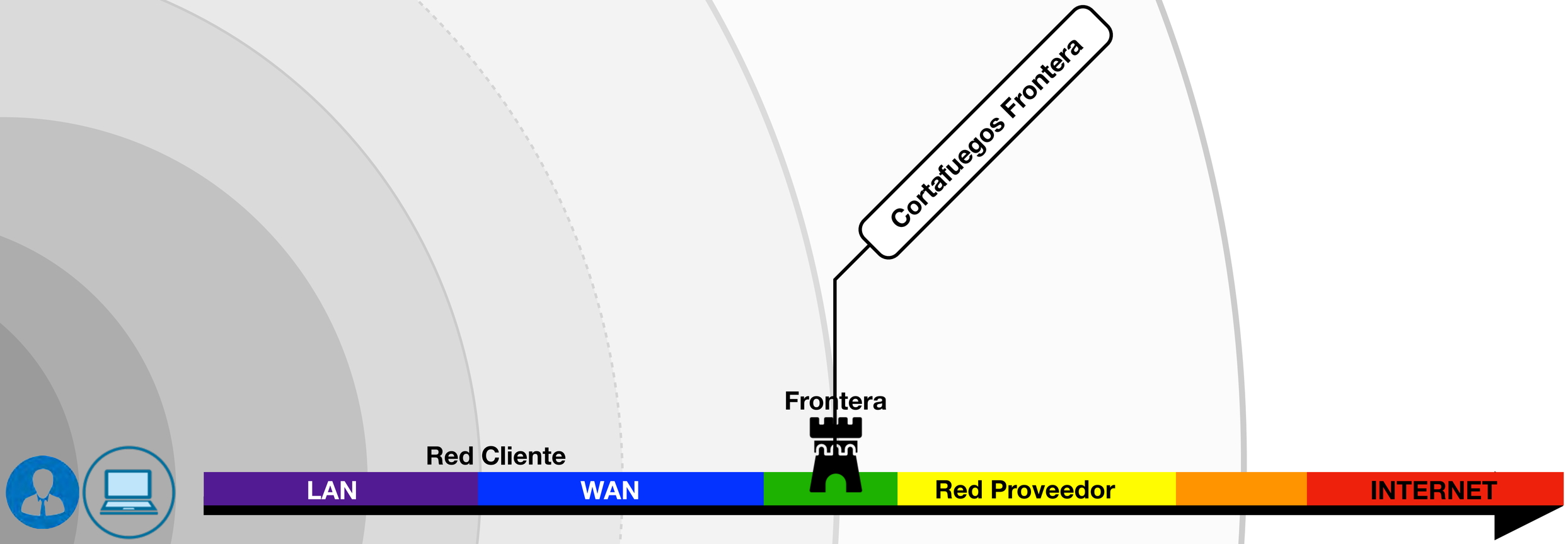

NIXVAL
46988 Paterna,
Valencia
Tránsito
Tata
Tránsito
Telia
Parque Tecnológico ,
Edif. 605. 48160. Derio
C/ Albasanz, 71.
28037 Madrid
amazon
web services
Office 365
Azure
Peering
CatNIx
DO NOT CROSS
Zamudio
Parque Tecnológico
Peering
EspanIx
C /Pablo Iglesias, 56
08908 L'Hospitalet de
Llobregat
Parque Tecnológico ,
Edif. 206. 48170. Zamudio
C/ Acer, 30-32,
08038 Barcelona
C/Mesena 80
28033
Parque Tecnológico ,
Edif. 103. 48170. Zamudio
Tránsito
Cogent
Peering
AmsIx


Base de Datos
Big Data
Recolector
de Flujos
NetFlow
Routers
Frontera
Servidores
Ventana Cliente
Base de Datos
Reglas de Corte
FlowSpec
Servidor BGP
FlowSpec

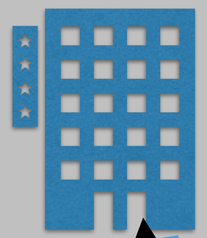

ventana-devel4.sarenet.es
sarenet
Redes
Dominios
javi@sarenet.es
ES
Circuitos
San Adrian
[1G]
Defensa perimetral
TCP
UDP
ESP
ICMP
GRE
93,9%
Tráfico en bits por segundo
4/10/2018, 2:19:52 PM - 4/11/2018, 2:19:52 PM
400M
300M
200M
100M
0
10/4 16:00
10/4 20:00
11/4 00:00
11/4 04:00
11/4 08:00
11/4 12:00
Flujo de paquetes por segundo
60k
50k
40k
30k
20k
10k
0
10/4 16:00
10/4 20:00
11/4 00:00
11/4 04:00
11/4 08:00
11/4 12:00
TCP 443
TCP 80
TCP 554
TCP 3101
TCP 25
TCP 58660
TCP 50040
TCP 53335
TCP 8292
TCP 51074
92,53Mbps
46,26Mbps
0bps
141.38.2.22
155.56.210.43
13.107.4.50
140.172.138.18
80.78.5.225
193.61.196.107
172.217.16.238
90.160.61.5
17.248.149.76
216.58.201.142
18,51Mbps
9,25Mbps
0bps
217.22.96.144
217.22.96.143
217.22.96.73
217.22.96.72
217.22.97.98
217.22.96.145
217.22.96.27
217.22.96.146
217.22.97.4
217.22.96.24
0bps
46,26Mbps
TCP 443
TCP 22
TCP 25
TCP 8443
TCP 44158
TCP 24292
TCP 63532
TCP 58539
TCP 23219
TCP 56780
0bps
4,63Mbps
9,25Mbps

Defensa Perimetral



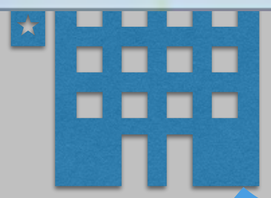

Cortafuegos Frontera
Frontera
Red Cliente
LAN
WAN
Red Proveedor
INTERNET

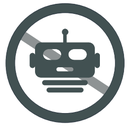
Cortafuegos Frontera



Red Privada Virtual

NSE CERTIFICATIONS								
	SALES			TECHNICAL				
	NSE 1	NSE 2	NSE 3	NSE 4	NSE 5	NSE 6	NSE 7	NSE 8
Required	2	2	1	3	3	1	2	0
Number Met	5	4	3	3	3	4	2	0





Anti-botnet

Intrusion Prevention

ntivirus

ulnerability
lanagement

Anti-spam

Web Filtering

IP Reputation

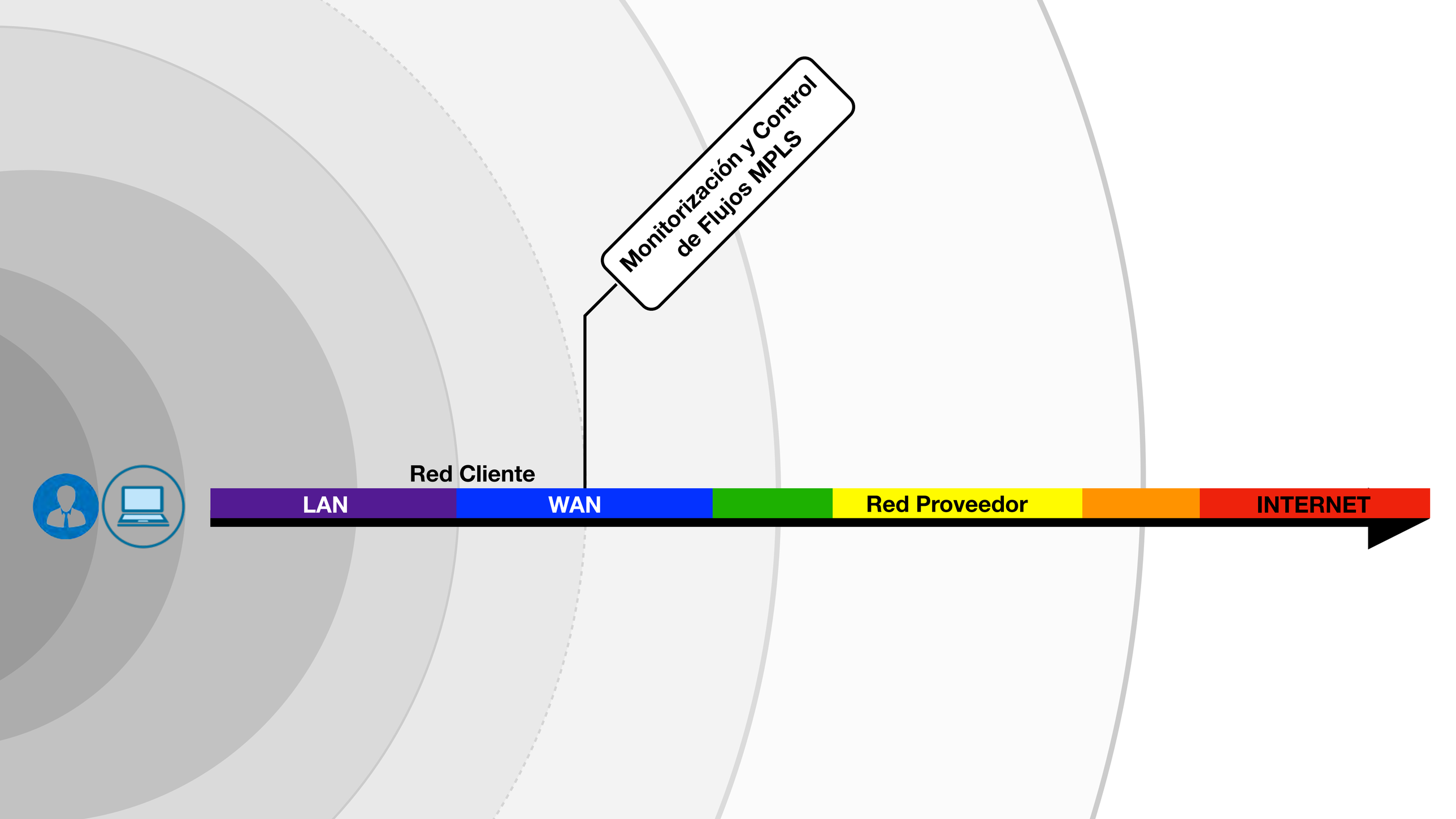
Application Control

Web Application Security

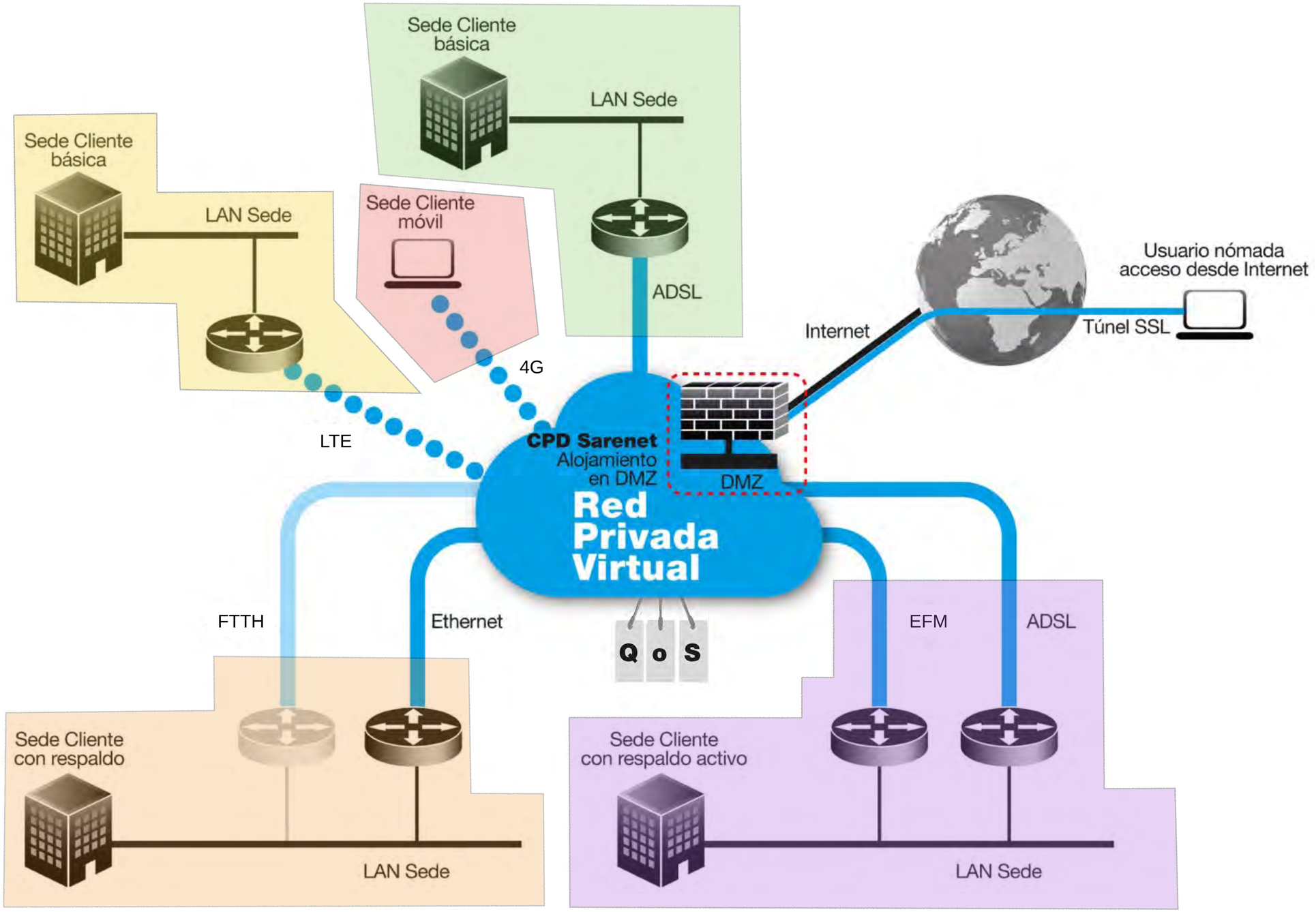
Advanced Threat Protection

Database Protection

Industrial Security Service


Monitorización y Control
de Flujos MPLS
Red Cliente
LAN
WAN
Red Proveedor
INTERNET

Control de Flujos MPLS


Sede Cliente básica
LAN Sede
Sede Cliente básica
LAN Sede
Sede Cliente móvil
ADSL
Usuario nómada acceso desde Internet
Internet
Túnel SSL
4G
LTE
CPD Sarenet
Alojamiento en DMZ
DMZ
Red Privada Virtual
FTTH
Ethernet
Q o S
EFM
ADSL
Sede Cliente con respaldo
LAN Sede
Sede Cliente con respaldo activo
LAN Sede

sarenet

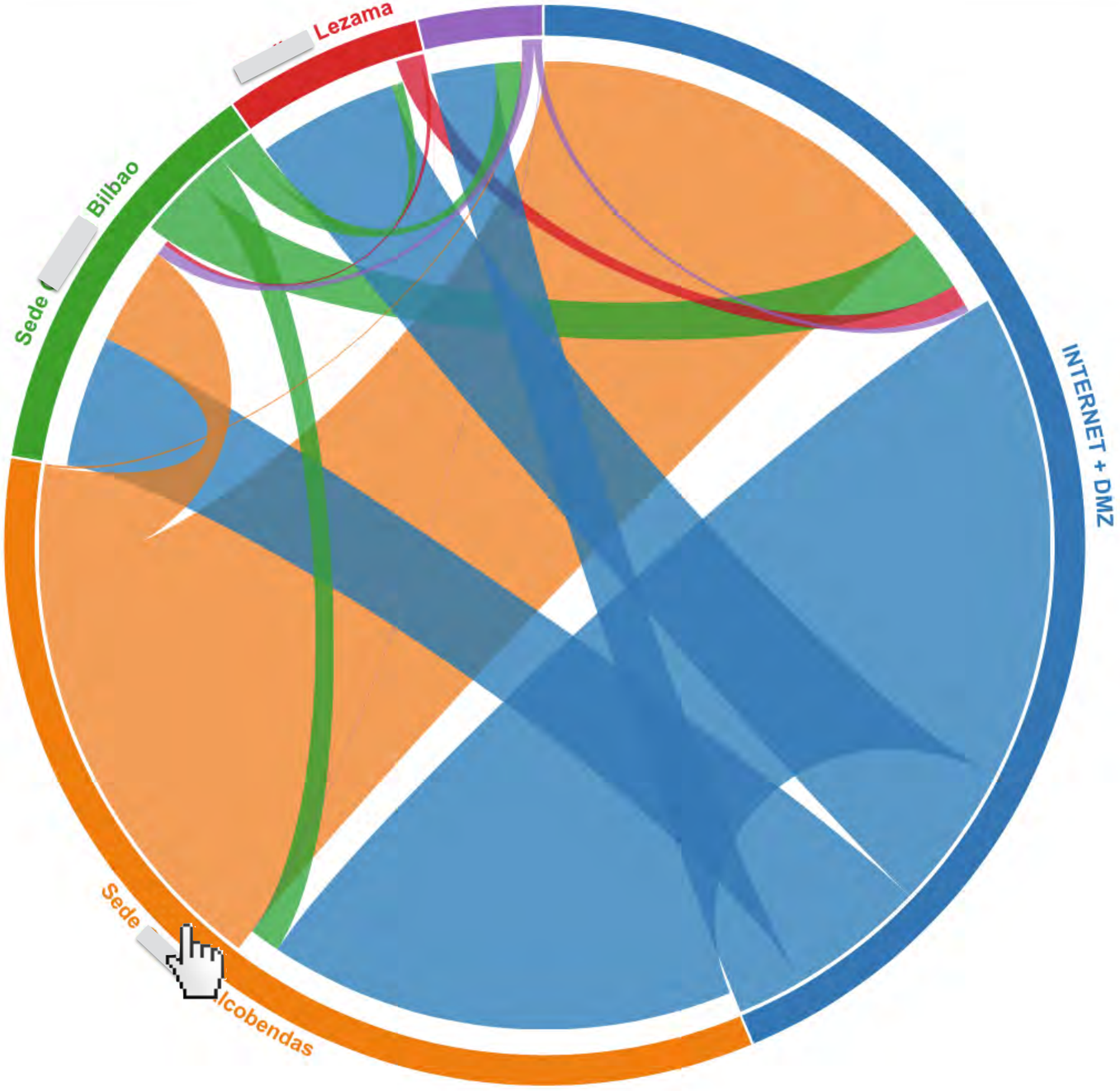
Descriptor: MPLS [redacted]

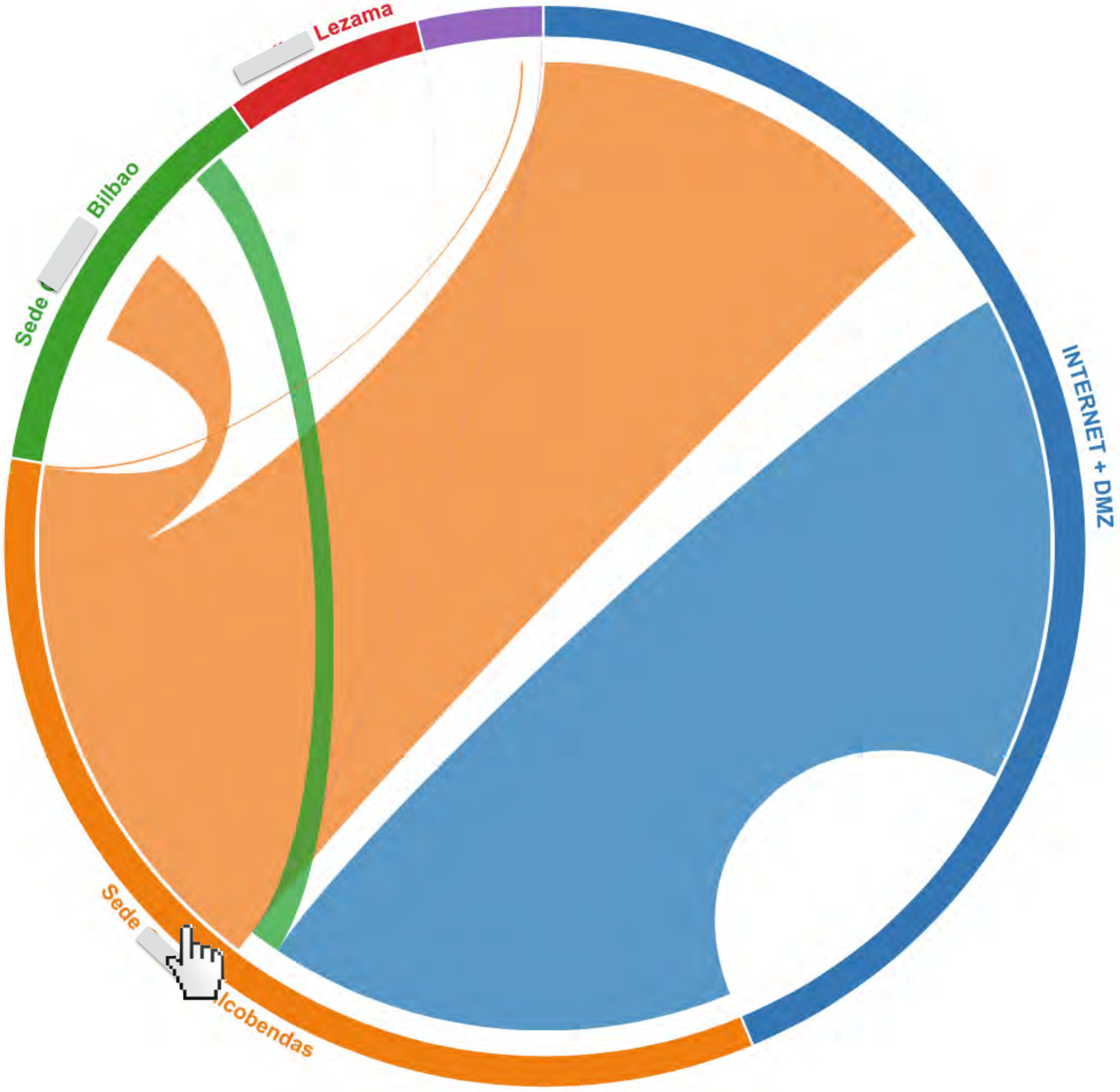
Tipo	QoS	Caudal Internet	Direcciones IP
MPLS	Datos-Sarepbx	100 Mbps	• 194.30.40.10/31 • 194.30.40.64/32

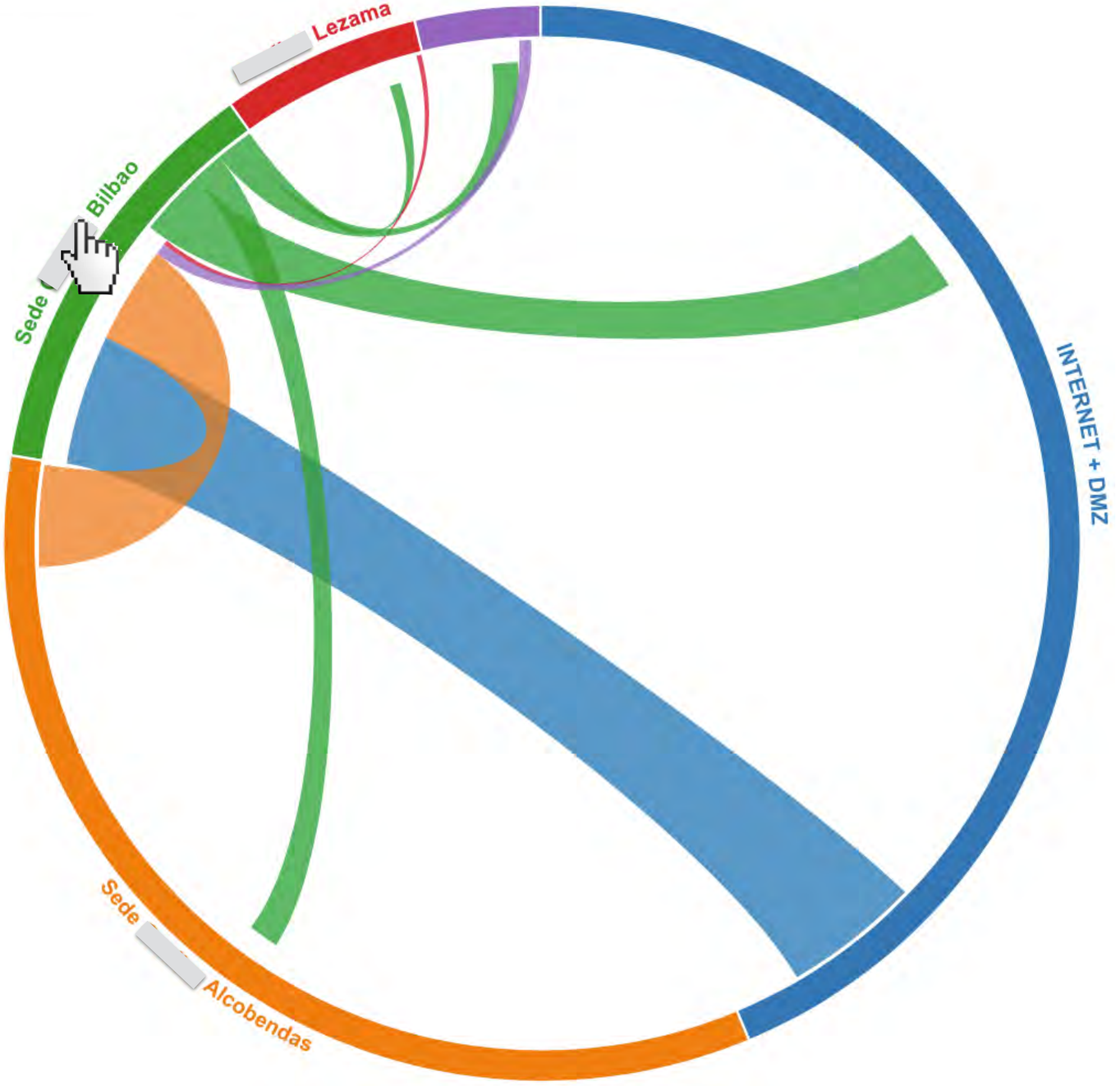
24/10/2017 12:18 - 25/10/2017 12:18

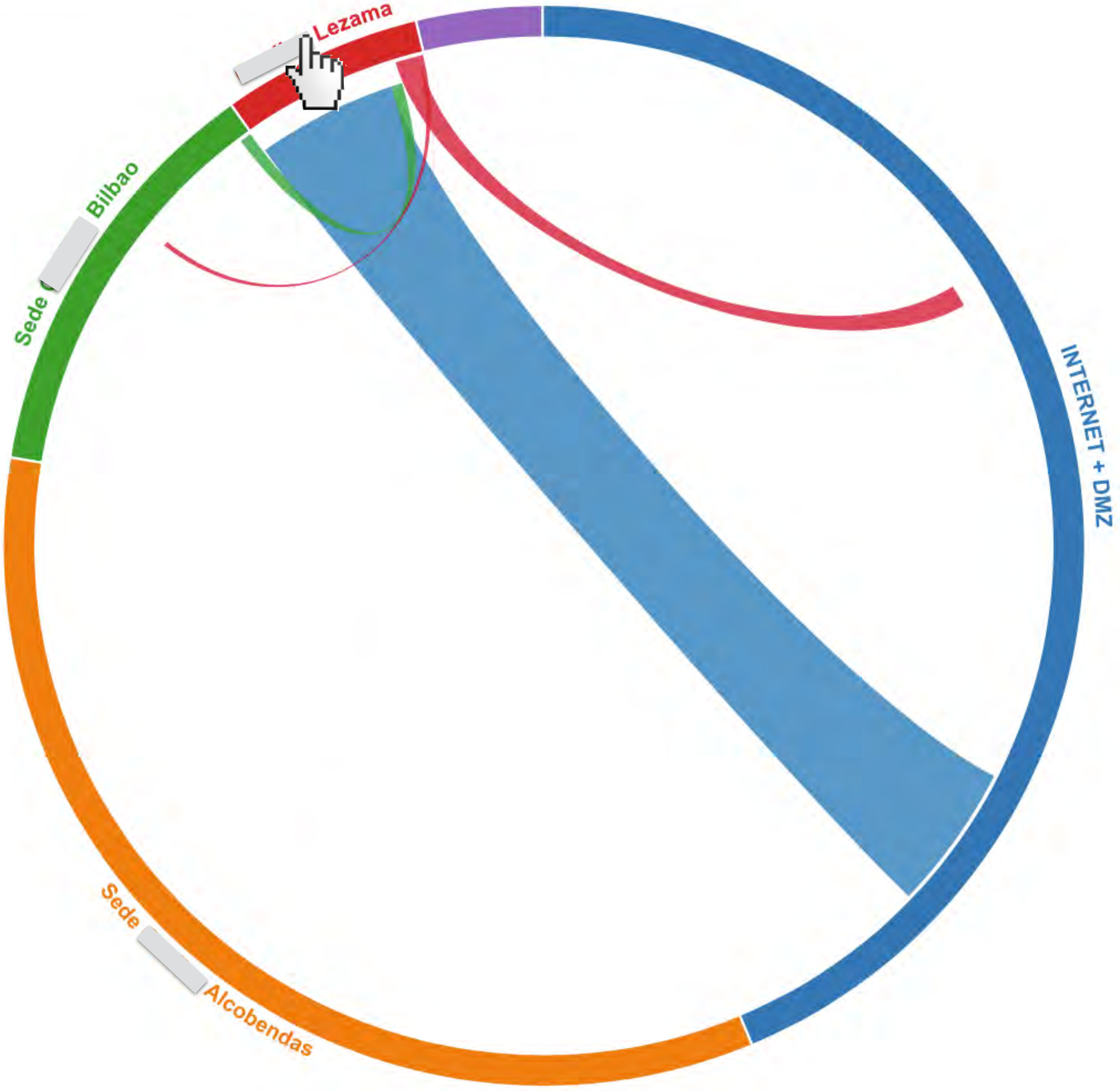
FILTRAR

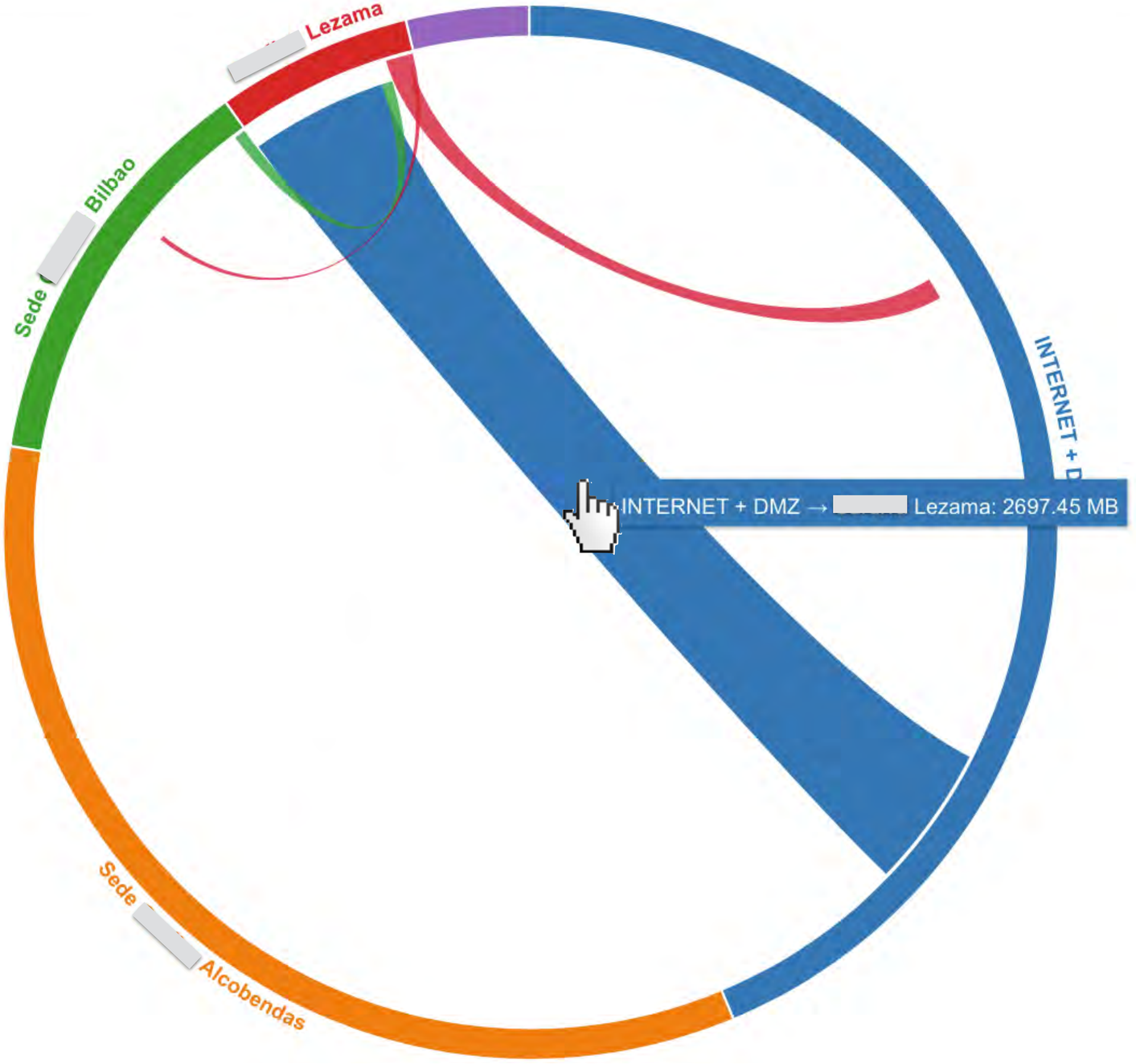
- INTERNET + DMZ
- Sede [redacted] Alcobendas [300M/300M - Backup]
- Sede [redacted] Bilbao [20M/20M - 10M/800k]
- [redacted] Lezama [10M/10M - Backup]
- Sede [redacted] Barcelona [30M/30M - Backup]
- [redacted] Lezama [100M/100M]

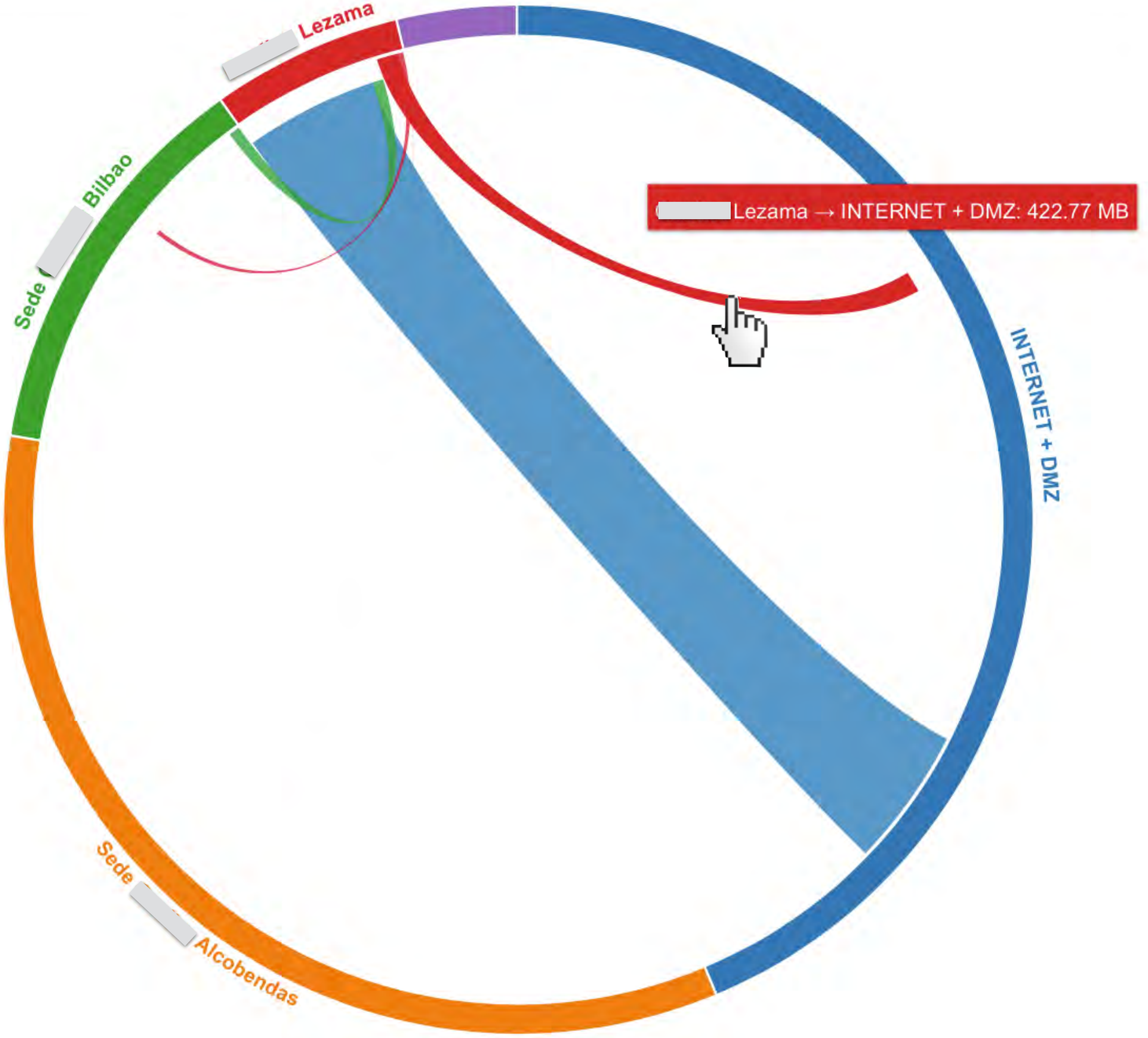

Lezama
Bilbao
Sede
INTERNET + DMZ
Sede
Alcobendas

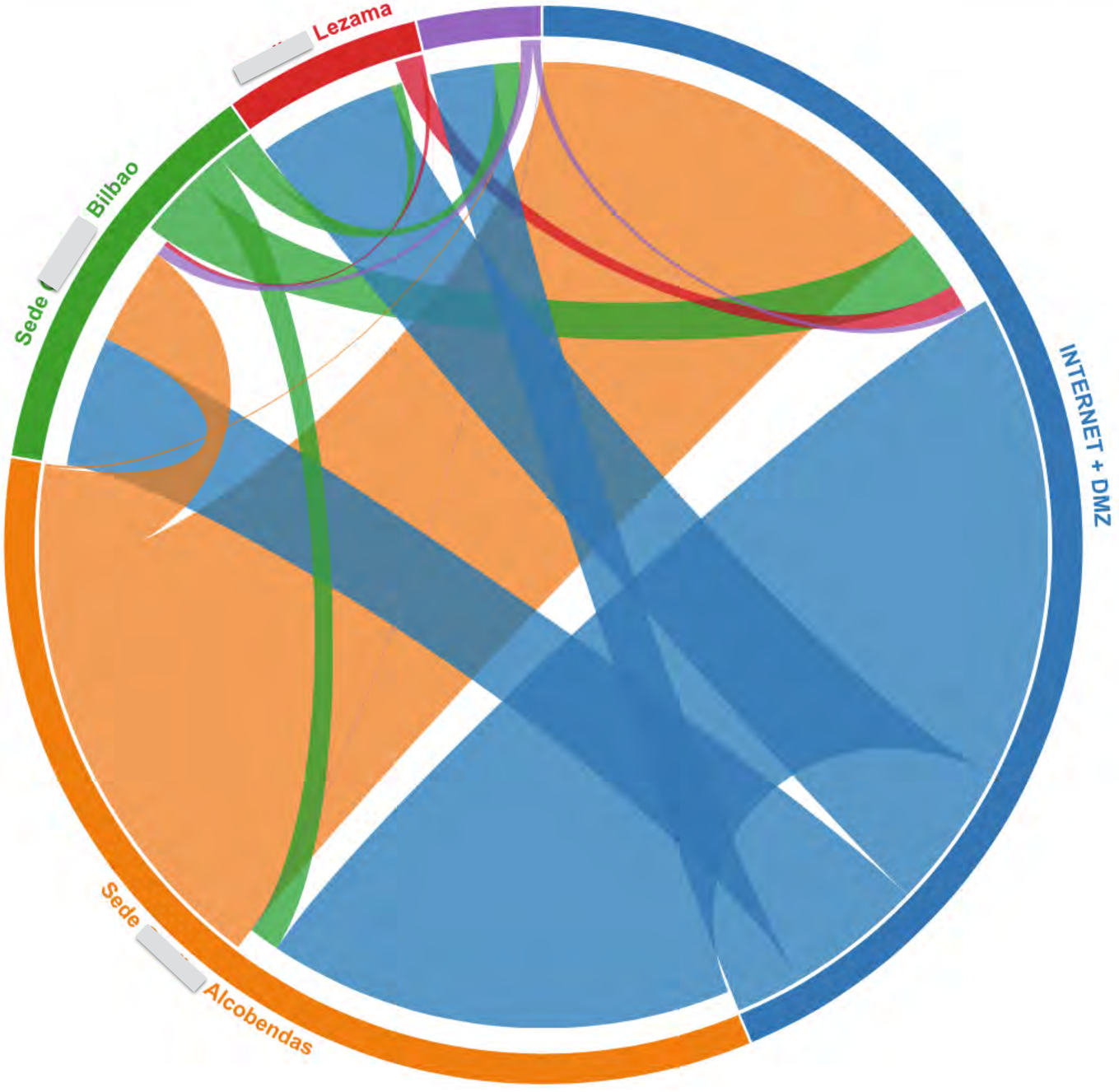

Lezama
Bilbao
Sede
INTERNET + DMZ
Sede
Alcobendas


Lezama
Bilbao
INTERNET + DMZ
Alcobendas


Lezama
Bilbao
Sede
INTERNET + DMZ
Sede
Alcobendas


Lezama
Bilbao
Sede
INTERNET + D
INTERNET + DMZ → Lezama: 2697.45 MB
Sede
Alcobendas

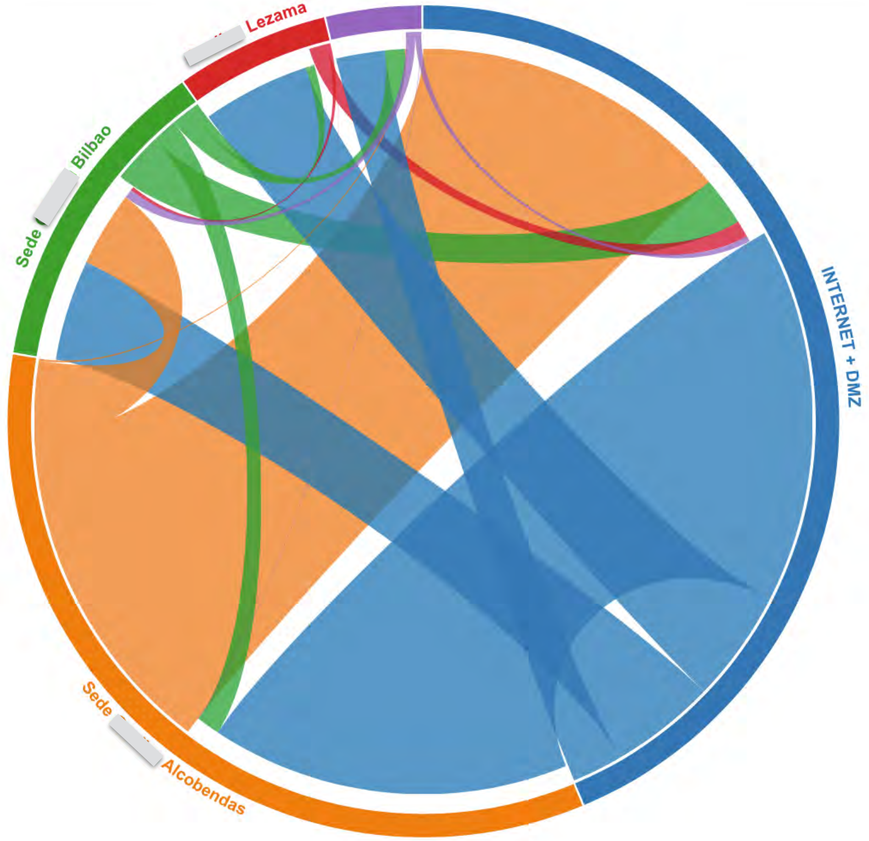

Lezama
Bilbao
Sede
Sede
Alcobendas
INTERNET + DMZ
Lezama → INTERNET + DMZ: 422.77 MB


Lezama
Bilbao
Sede
INTERNET + DMZ
Sede
Alcobendas

Descriptor: MPLS [redacted]

Tipo	QoS	Caudal Internet	Direcciones IP
MPLS	Datos-Sarepbx	100 Mbps	• 194.30.40.10/31 • 194.30.40.64/32

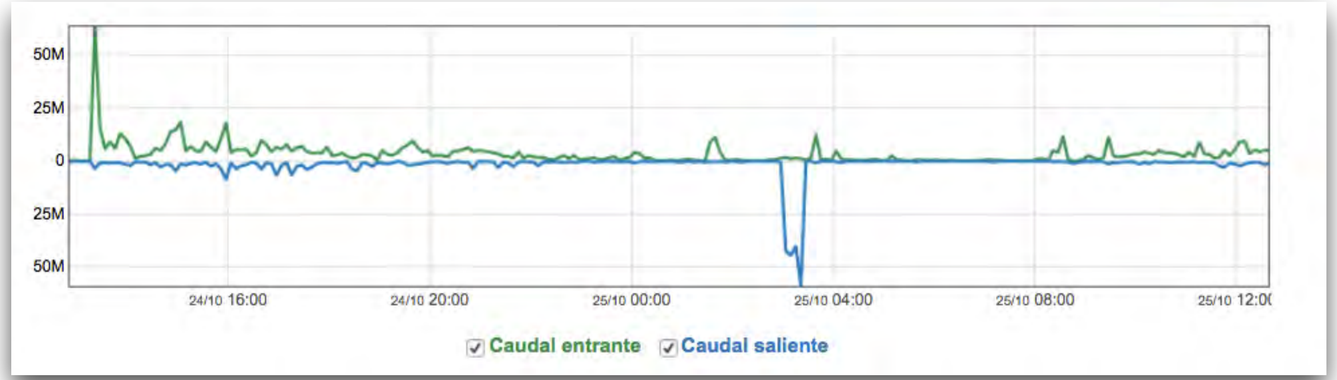
24/10/2017 12:18 - 25/10/2017 12:18

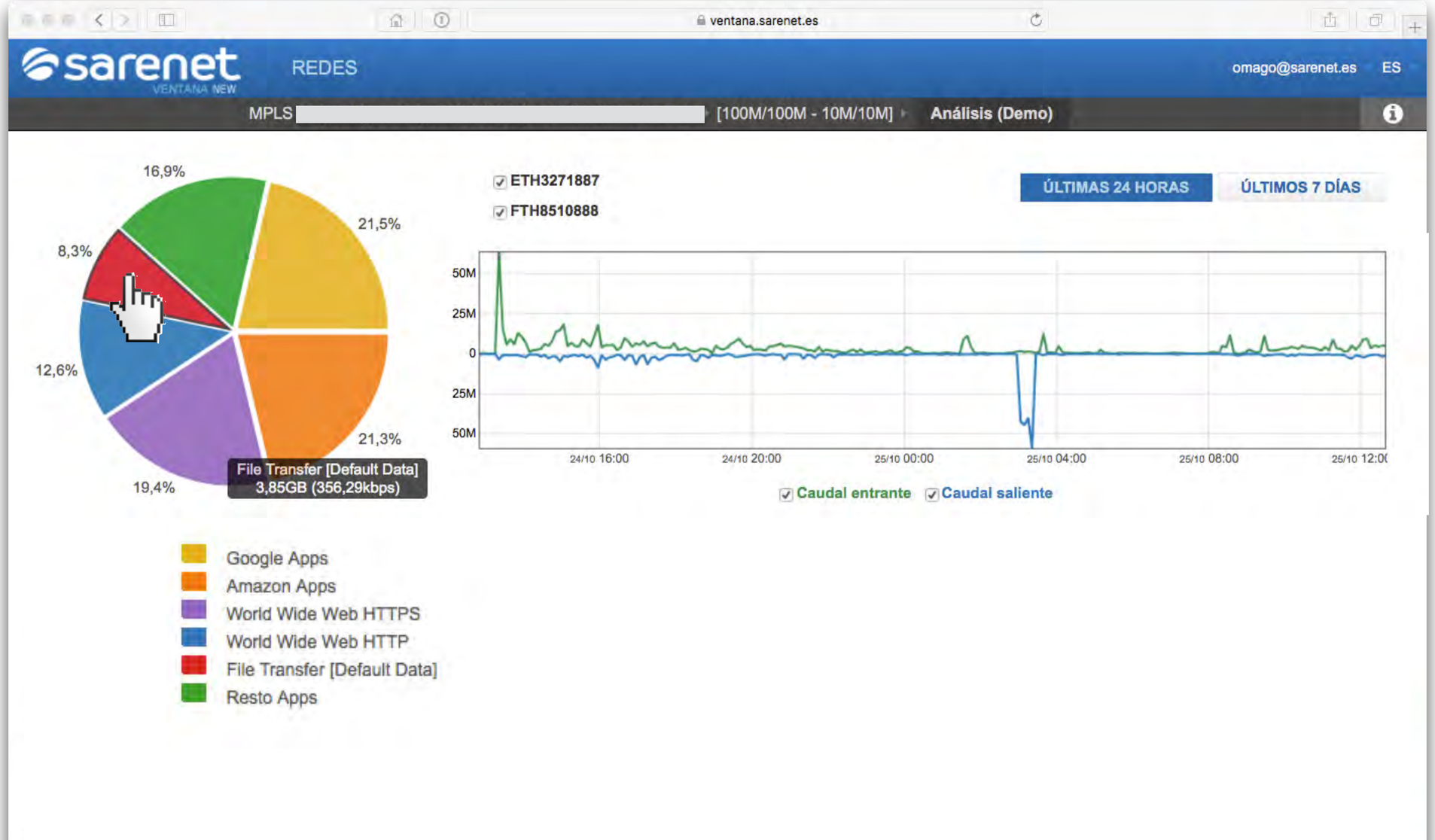


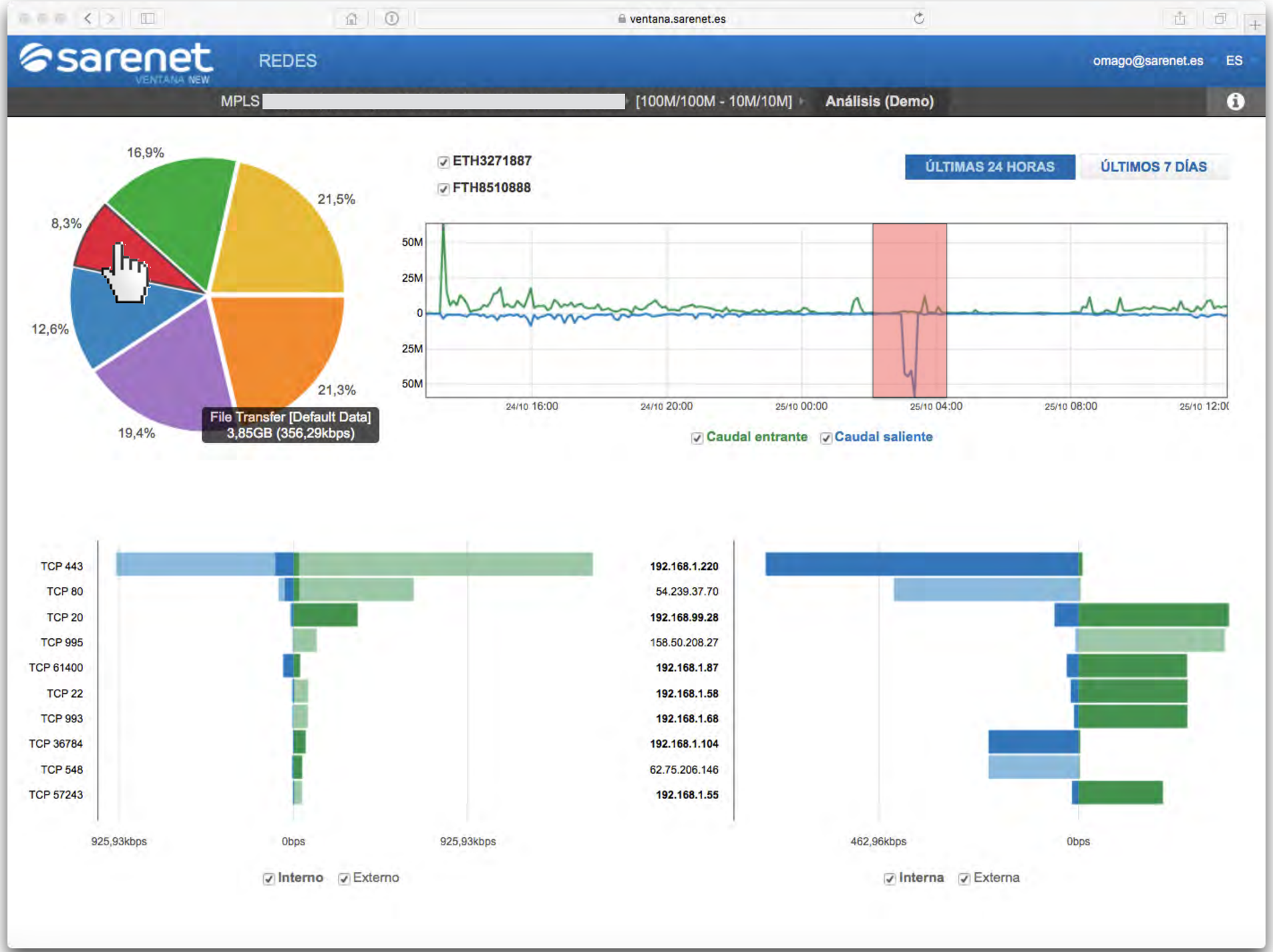
FILTRAR

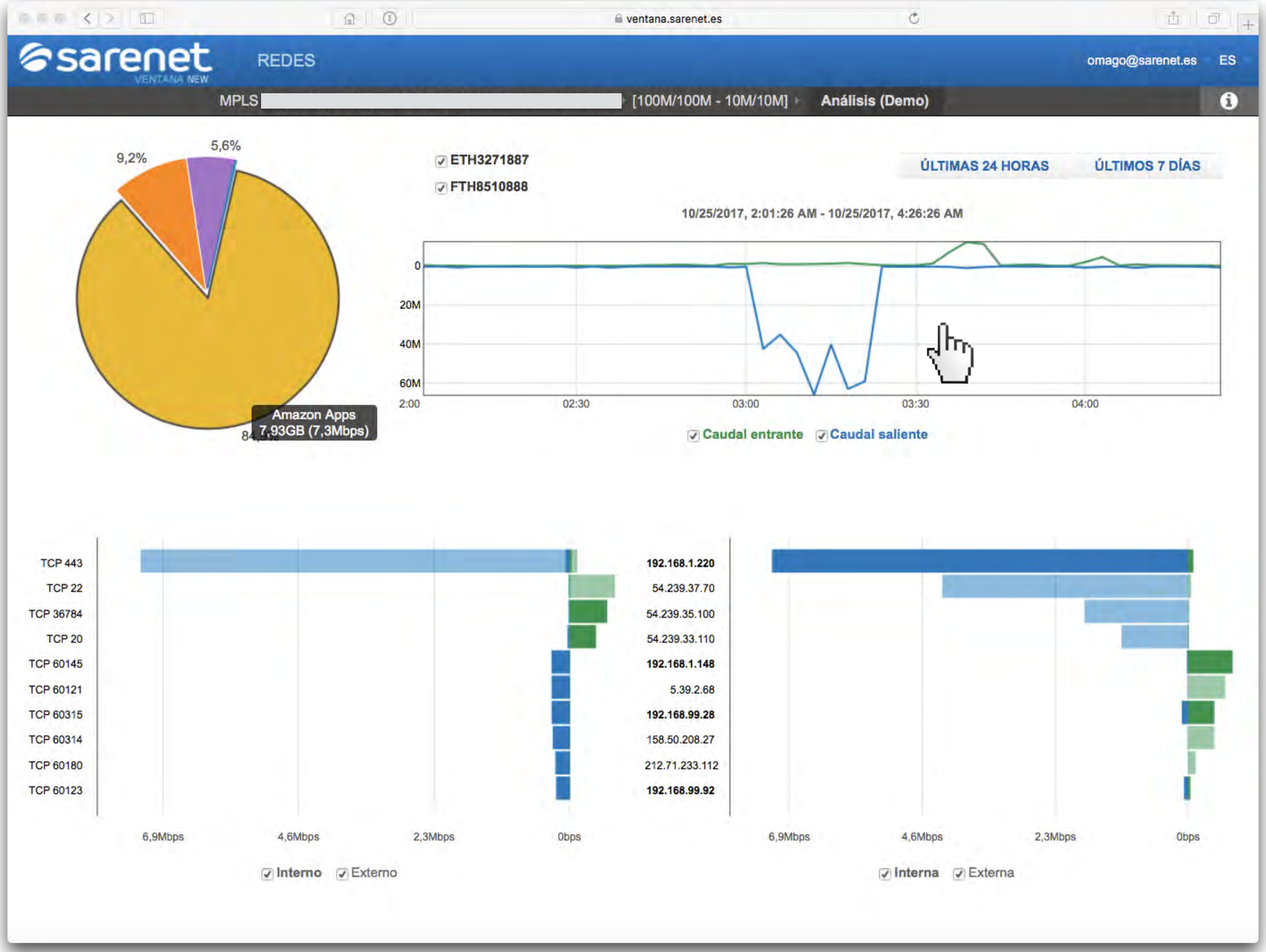
- INTERNET + DMZ
- Sede [redacted] Alcobendas [300M/300M - Backup]
- Sede [redacted] Bilbao [20M/20M - 10M/800k]
- [redacted] Lezama [10M/10M - Backup]
- Sede [redacted] Barcelona [30M/30M - Backup]
- [redacted] Lezama [100M/100M]

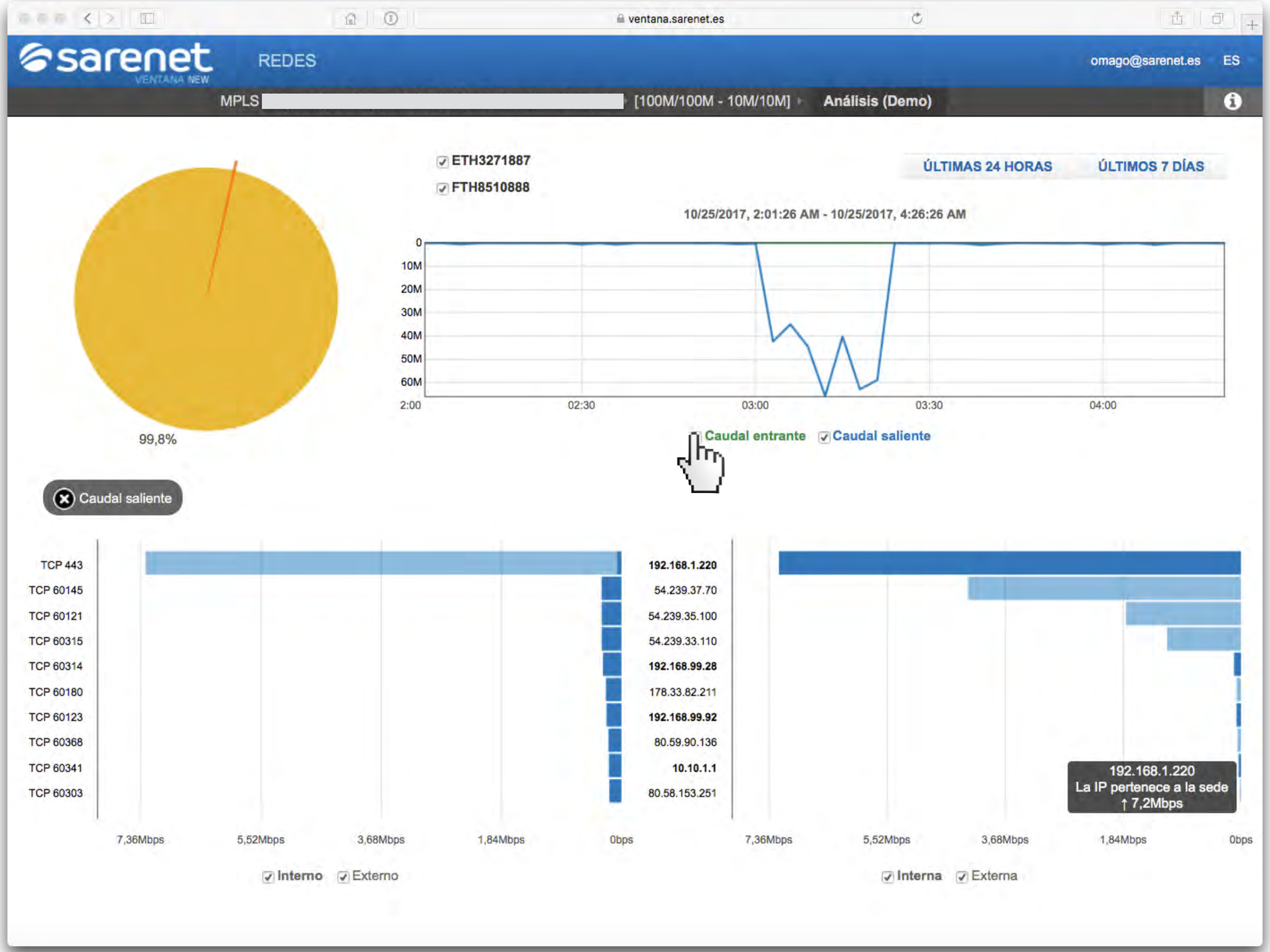
Sede [redacted] Bilbao

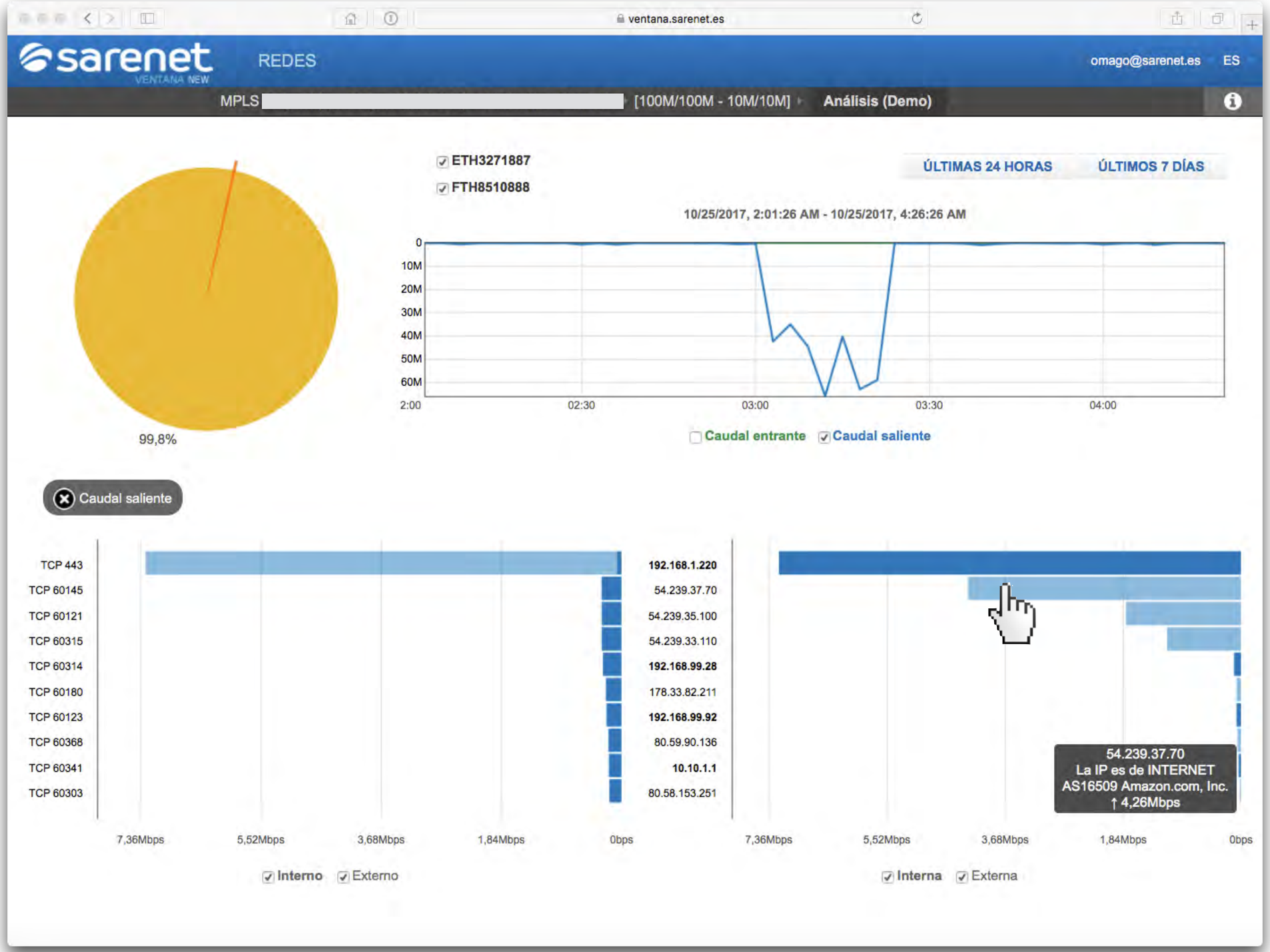


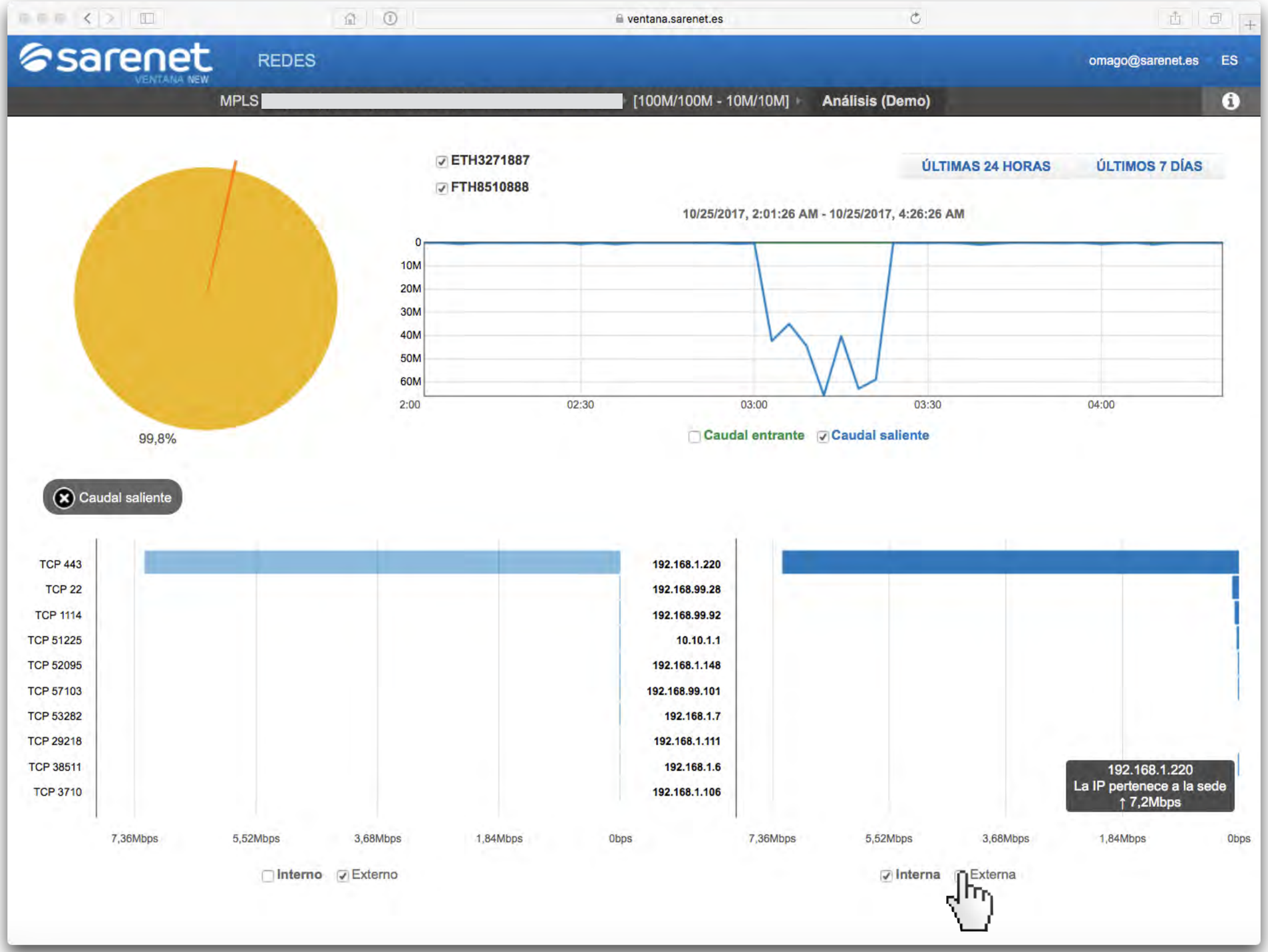

ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
16,9%
21,5%
8,3%
12,6%
21,3%
19,4%
File Transfer [Default Data]
3,85GB (356,29kbps)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
50M
25M
0
25M
50M
24/10 16:00
24/10 20:00
25/10 00:00
25/10 04:00
25/10 08:00
Caudal entrante
Caudal saliente
Google Apps
Amazon Apps
World Wide Web HTTPS
World Wide Web HTTP
File Transfer [Default Data]
Resto Apps

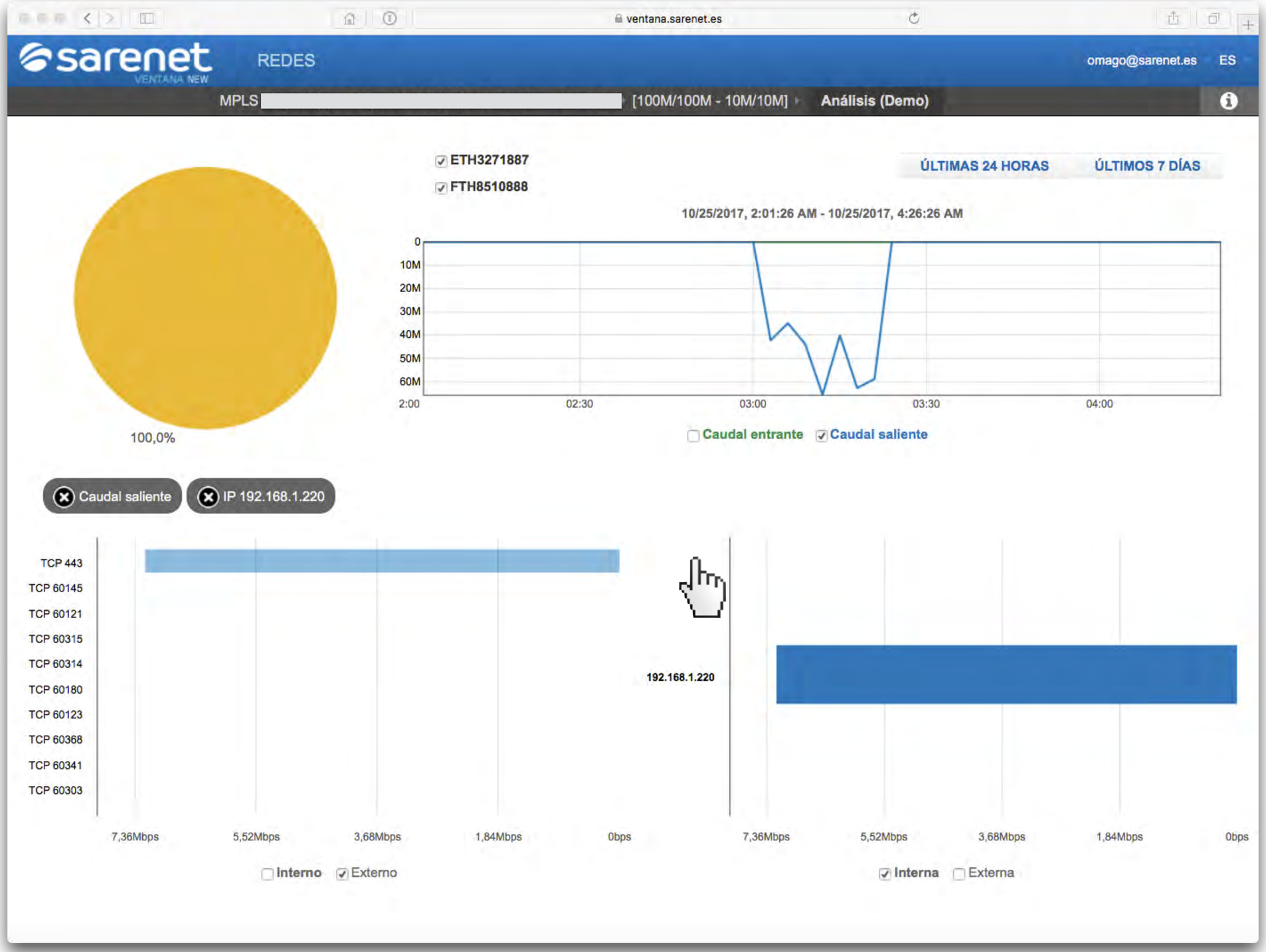

ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
16,9%
21,5%
8,3%
12,6%
21,3%
19,4%
File Transfer [Default Data]
3,85GB (356,29kbps)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
50M
25M
0
25M
50M
24/10 16:00
24/10 20:00
25/10 00:00
25/10 04:00
25/10 08:00
25/10 12:0
Caudal entrante
Caudal saliente
TCP 443
TCP 80
TCP 20
TCP 995
TCP 61400
TCP 22
TCP 993
TCP 36784
TCP 548
TCP 57243
192.168.1.220
54.239.37.70
192.168.99.28
158.50.208.27
192.168.1.87
192.168.1.58
192.168.1.68
192.168.1.104
62.75.206.146
192.168.1.55
925,93kbps
0bps
925,93kbps
462,96kbps
0bps
Interno
Externo
Interna
Externa

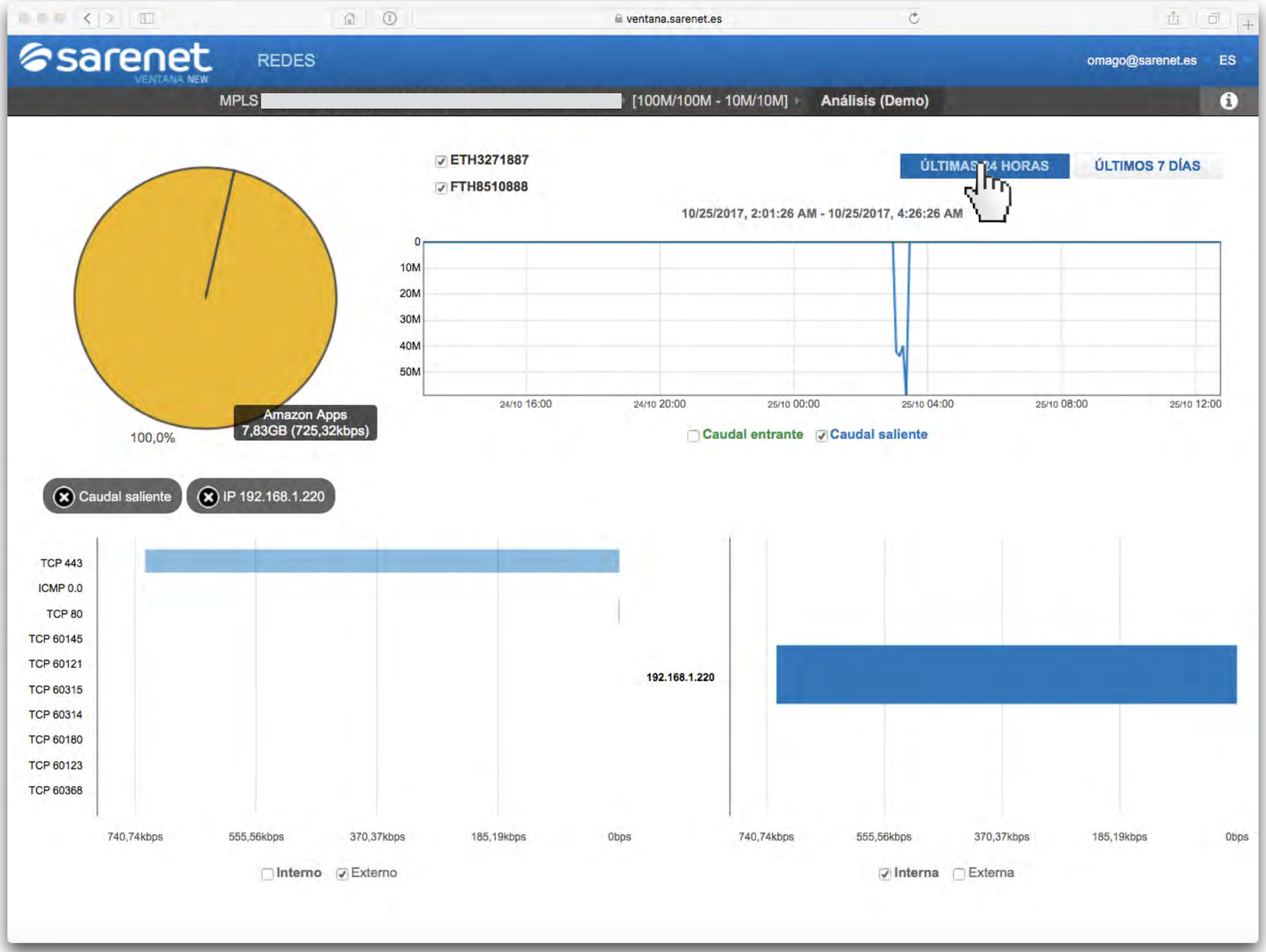

ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
9,2%
5,6%
Amazon Apps
7,93GB (7,3Mbps)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
10/25/2017, 2:01:26 AM - 10/25/2017, 4:26:26 AM
0
20M
40M
60M
2:00
02:30
03:00
03:30
04:00
Caudal entrante
Caudal saliente
TCP 443
TCP 22
TCP 36784
TCP 20
TCP 60145
TCP 60121
TCP 60315
TCP 60314
TCP 60180
TCP 60123
192.168.1.220
54.239.37.70
54.239.35.100
54.239.33.110
192.168.1.148
5.39.2.68
192.168.99.28
158.50.208.27
212.71.233.112
192.168.99.92
6,9Mbps
4,6Mbps
2,3Mbps
0bps
Interno
Externo
6,9Mbps
4,6Mbps
2,3Mbps
0bps
Interna
Externa

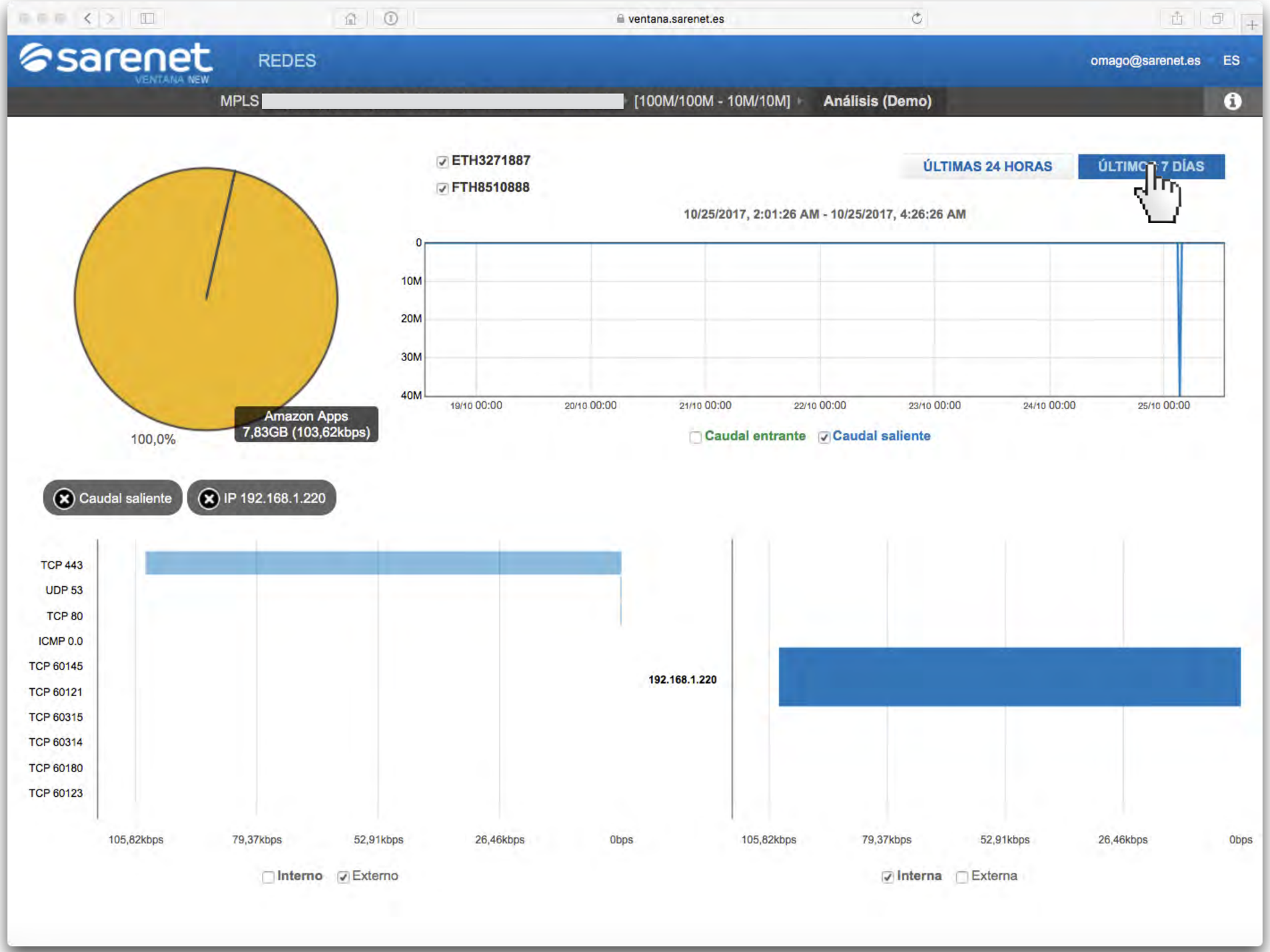

ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
10/25/2017, 2:01:26 AM - 10/25/2017, 4:26:26 AM
0
10M
20M
30M
40M
50M
60M
2:00
02:30
03:00
03:30
04:00
99,8%
Caudal entrante
Caudal saliente
Caudal saliente
TCP 443
TCP 60145
TCP 60121
TCP 60315
TCP 60314
TCP 60180
TCP 60123
TCP 60368
TCP 60341
TCP 60303
192.168.1.220
54.239.37.70
54.239.35.100
54.239.33.110
192.168.99.28
178.33.82.211
192.168.99.92
80.59.90.136
10.10.1.1
80.58.153.251
7,36Mbps
5,52Mbps
3,68Mbps
1,84Mbps
0bps
192.168.1.220
La IP pertenece a la sede
↑ 7,2Mbps
Interno
Externo
Interna
Externa

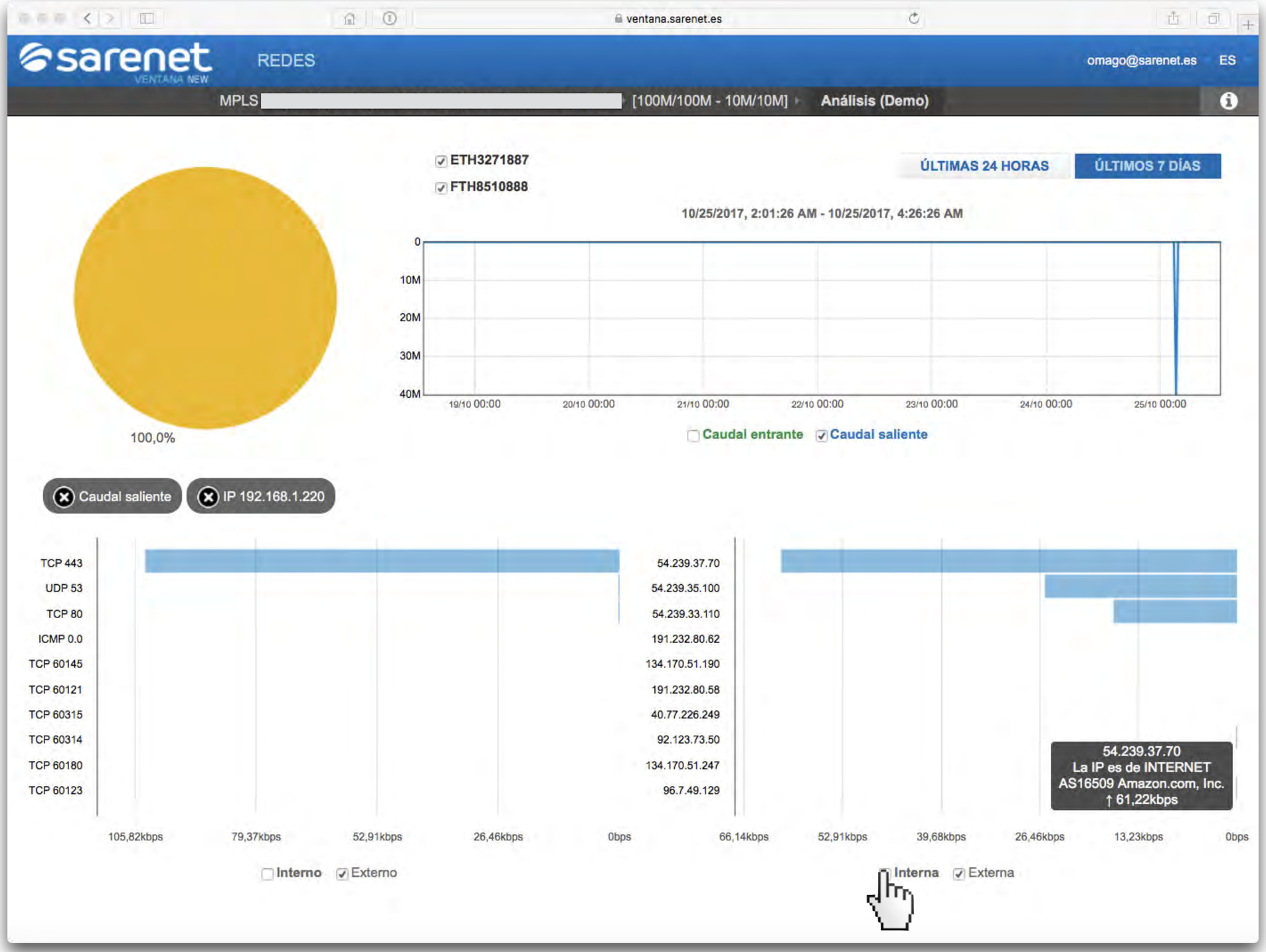

ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
10/25/2017, 2:01:26 AM - 10/25/2017, 4:26:26 AM
0
10M
20M
30M
40M
50M
60M
2:00
02:30
03:00
03:30
04:00
99,8%
Caudal entrante
Caudal saliente
Caudal saliente
TCP 443
TCP 60145
TCP 60121
TCP 60315
TCP 60314
TCP 60180
TCP 60123
TCP 60368
TCP 60341
TCP 60303
192.168.1.220
54.239.37.70
54.239.35.100
54.239.33.110
192.168.99.28
178.33.82.211
192.168.99.92
80.59.90.136
10.10.1.1
80.58.153.251
7,36Mbps
5,52Mbps
3,68Mbps
1,84Mbps
0bps
Interno
Externo
54.239.37.70
La IP es de INTERNET
AS16509 Amazon.com, Inc.
↑ 4,26Mbps
7,36Mbps
5,52Mbps
3,68Mbps
1,84Mbps
0bps
Interna
Externa

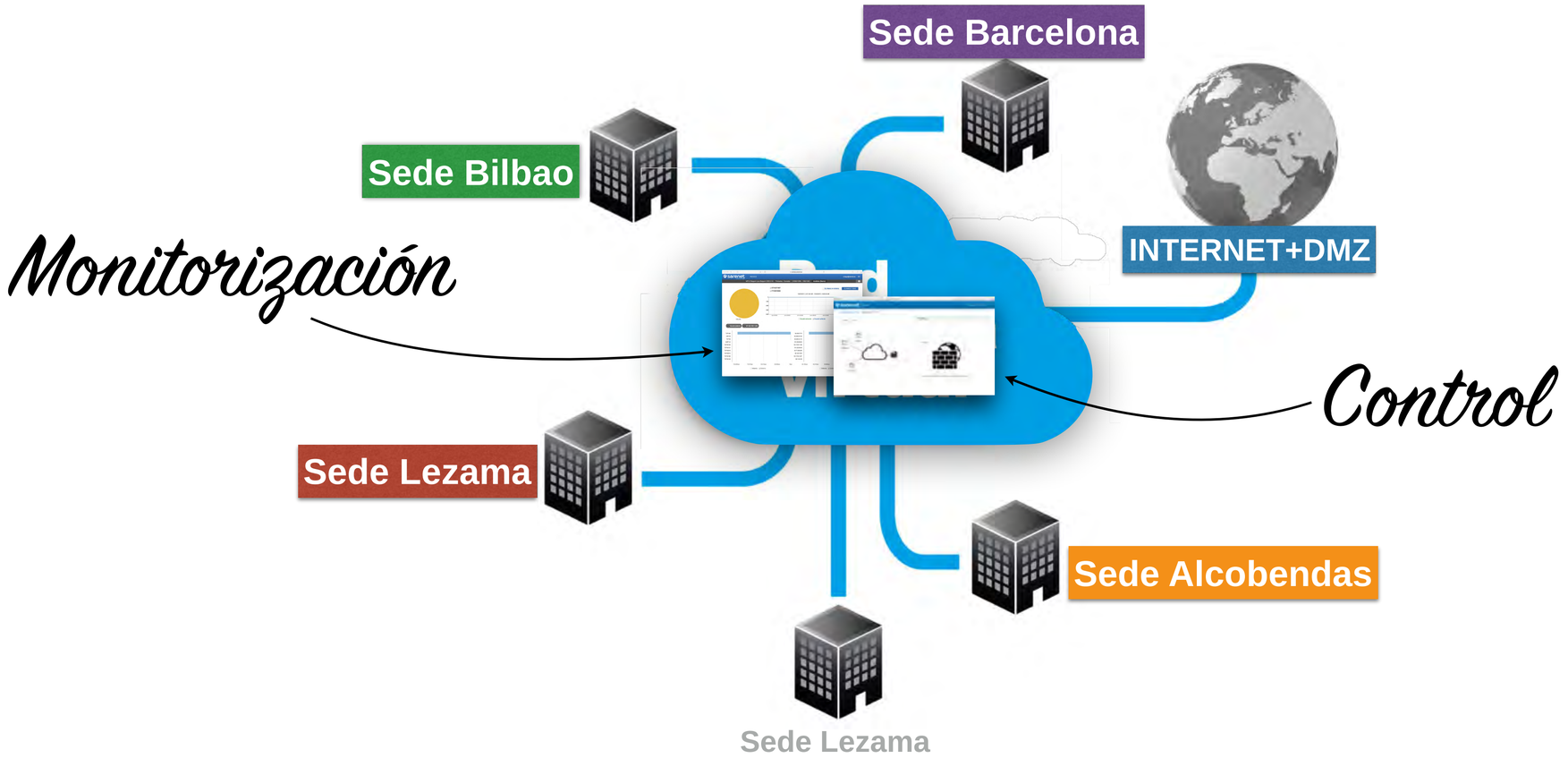

ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
10/25/2017, 2:01:26 AM - 10/25/2017, 4:26:26 AM
0
10M
20M
30M
40M
50M
60M
2:00
02:30
03:00
03:30
04:00
Caudal entrante
Caudal saliente
99,8%
Caudal saliente
TCP 443
TCP 22
TCP 1114
TCP 51225
TCP 52095
TCP 57103
TCP 53282
TCP 29218
TCP 38511
TCP 3710
192.168.1.220
192.168.99.28
192.168.99.92
10.10.1.1
192.168.1.148
192.168.99.101
192.168.1.7
192.168.1.111
192.168.1.6
192.168.1.106
192.168.1.220
La IP pertenece a la sede
↑ 7,2Mbps
7,36Mbps
5,52Mbps
3,68Mbps
1,84Mbps
0bps
Interno
Externo
Interna
Externa

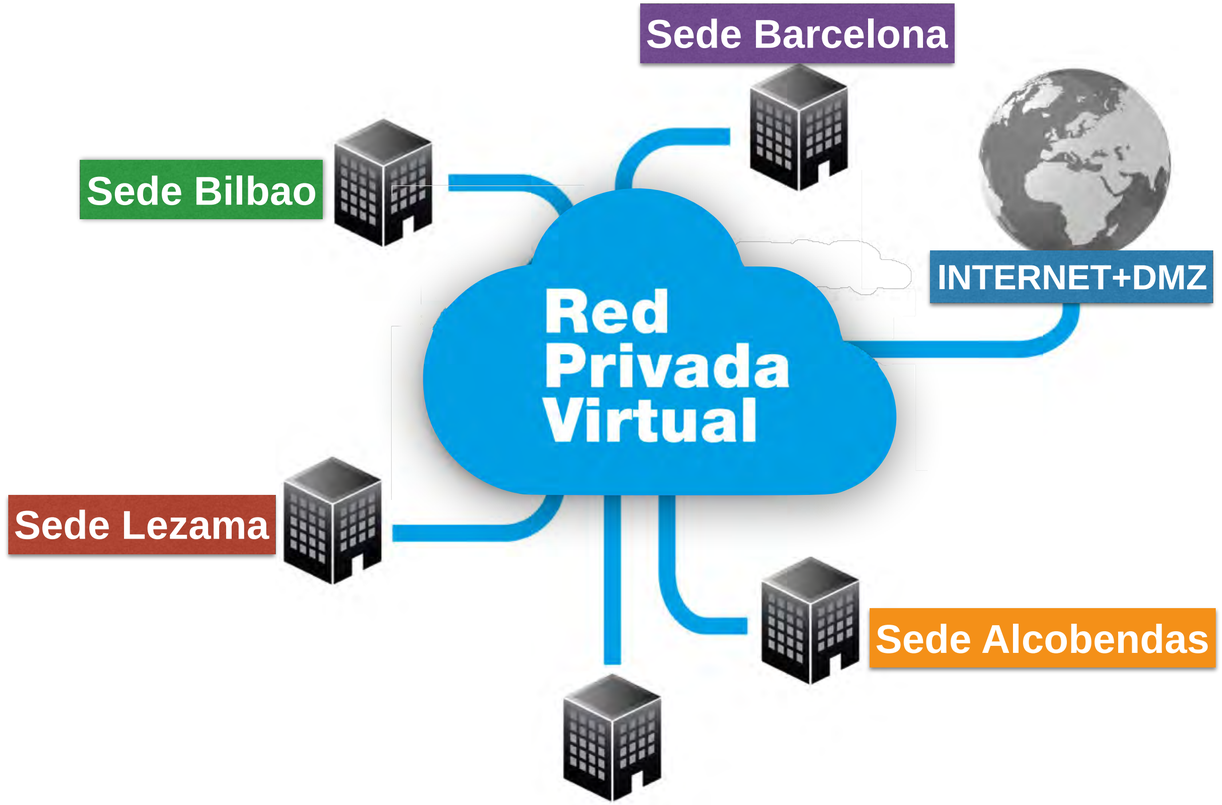

ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
10/25/2017, 2:01:26 AM - 10/25/2017, 4:26:26 AM
0
10M
20M
30M
40M
50M
60M
2:00
02:30
03:00
03:30
04:00
Caudal entrante
Caudal saliente
100,0%
Caudal saliente
IP 192.168.1.220
TCP 443
TCP 60145
TCP 60121
TCP 60315
TCP 60314
TCP 60180
TCP 60123
TCP 60368
TCP 60341
TCP 60303
192.168.1.220
7,36Mbps
5,52Mbps
3,68Mbps
1,84Mbps
0bps
Interno
Externo
Interna
Externa


ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
10/25/2017, 2:01:26 AM - 10/25/2017, 4:26:26 AM
0
10M
20M
30M
40M
50M
24/10 16:00
24/10 20:00
25/10 00:00
25/10 04:00
25/10 08:00
25/10 12:00
Caudal entrante
Caudal saliente
Amazon Apps
7,83GB (725,32kbps)
100,0%
Caudal saliente
IP 192.168.1.220
TCP 443
ICMP 0.0
TCP 80
TCP 60145
TCP 60121
TCP 60315
TCP 60314
TCP 60180
TCP 60123
TCP 60368
192.168.1.220
740,74kbps
555,56kbps
370,37kbps
185,19kbps
0bps
Interno
Externo
Interna
Externa


ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
10/25/2017, 2:01:26 AM - 10/25/2017, 4:26:26 AM
0
10M
20M
30M
40M
19/10 00:00
20/10 00:00
21/10 00:00
22/10 00:00
23/10 00:00
24/10 00:00
25/10 00:00
Caudal entrante
Caudal saliente
Amazon Apps
7,83GB (103,62kbps)
100,0%
Caudal saliente
IP 192.168.1.220
TCP 443
UDP 53
TCP 80
ICMP 0.0
TCP 60145
TCP 60121
TCP 60315
TCP 60314
TCP 60180
TCP 60123
192.168.1.220
105,82kbps
79,37kbps
52,91kbps
26,46kbps
0bps
Interno
Externo
Interna
Externa


ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
10/25/2017, 2:01:26 AM - 10/25/2017, 4:26:26 AM
0
10M
20M
30M
40M
19/10 00:00
20/10 00:00
21/10 00:00
22/10 00:00
23/10 00:00
24/10 00:00
25/10 00:00
Caudal entrante
Caudal saliente
100,0%
Caudal saliente
IP 192.168.1.220
TCP 443
UDP 53
TCP 80
ICMP 0.0
TCP 60145
TCP 60121
TCP 60315
TCP 60314
TCP 60180
TCP 60123
54.239.37.70
54.239.35.100
54.239.33.110
191.232.80.62
134.170.51.190
191.232.80.58
40.77.226.249
92.123.73.50
134.170.51.247
96.7.49.129
54.239.37.70
La IP es de INTERNET
AS16509 Amazon.com, Inc.
↑ 61,22kbps
105,82kbps
79,37kbps
52,91kbps
26,46kbps
0bps
66,14kbps
52,91kbps
39,68kbps
26,46kbps
13,23kbps
0bps
Interno
Externo
Interna
Externa


Sede Barcelona
Sede Bilbao
Monitorización
INTERNET+DMZ
Control
Sede Lezama
Sede Alcobendas
Sede Lezama


Sede Barcelona
Sede Bilbao
INTERNET+DMZ
Red
Privada
Virtual
Sede Lezama
Sede Alcobendas
Sede Lezama

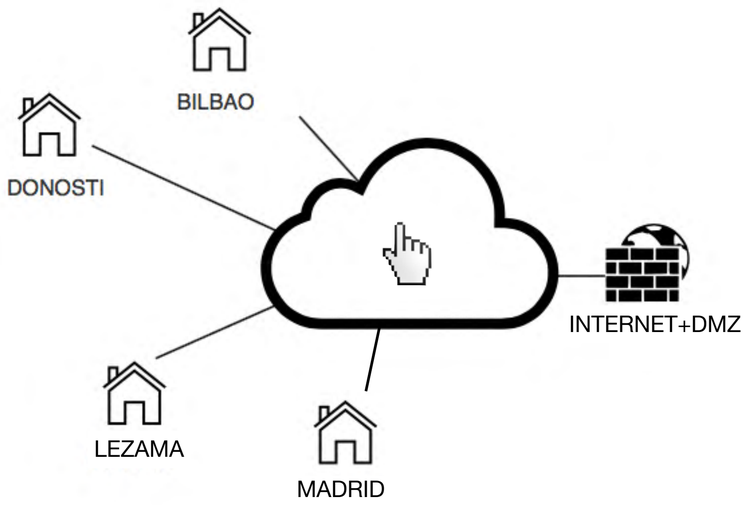
ventana.sarenet.es

sarenet Redes

omago@sarenet.es ES

MPLS DEMO » IS-MPLS-FW

Sedes Rosco



POLÍTICA

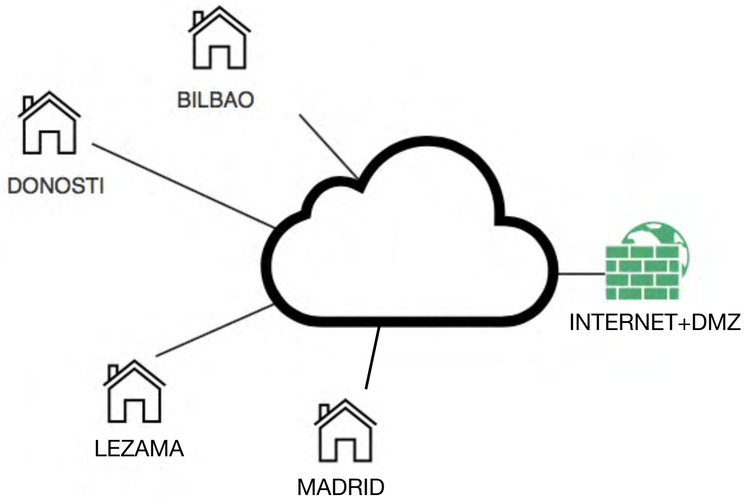
ventana.sarenet.es

sarenet Redes

omago@sarenet.es ES

MPLS DEMO » IS-MPLS-FW

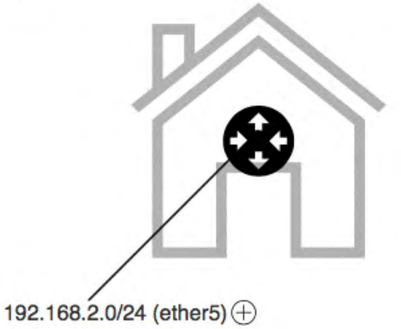
Sedes Rosco



POLÍTICA

Frontera

BILBAO (FTH1825614-MOV3755892)



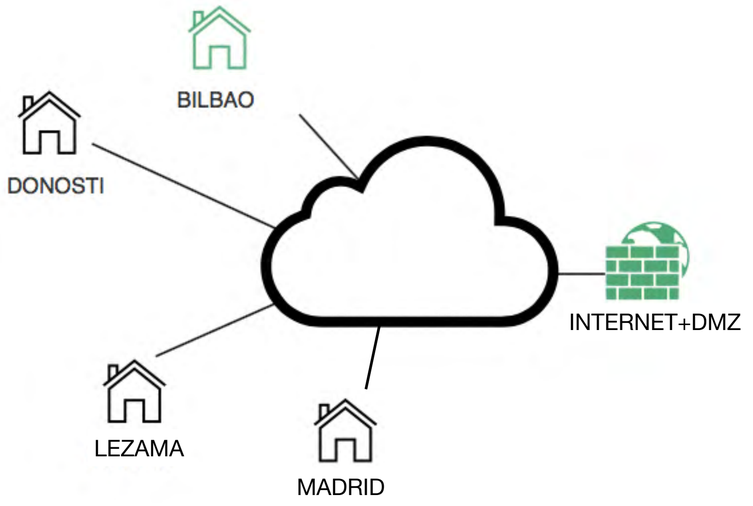
ventana.sarenet.es

sarenet Redes

omago@sarenet.es ES

MPLS DEMO » IS-MPLS-FW

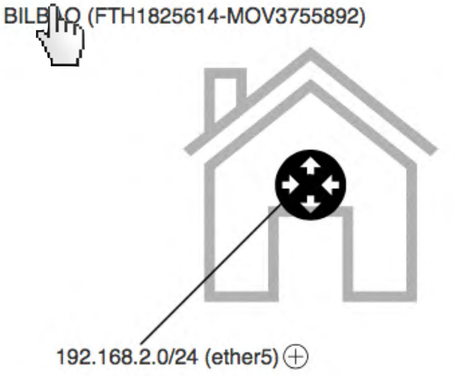
Sedes Rosco



POLÍTICA

Frontera

BILBAO



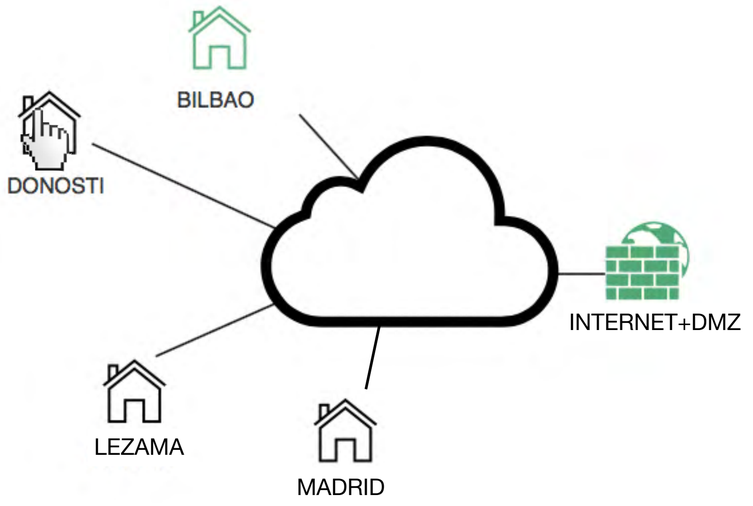
ventana.sarenet.es

sarenet Redes

omago@sarenet.es ES

MPLS DEMO » IS-MPLS-FW

Sedes Rosco

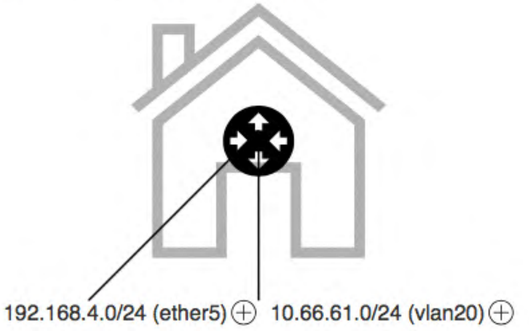


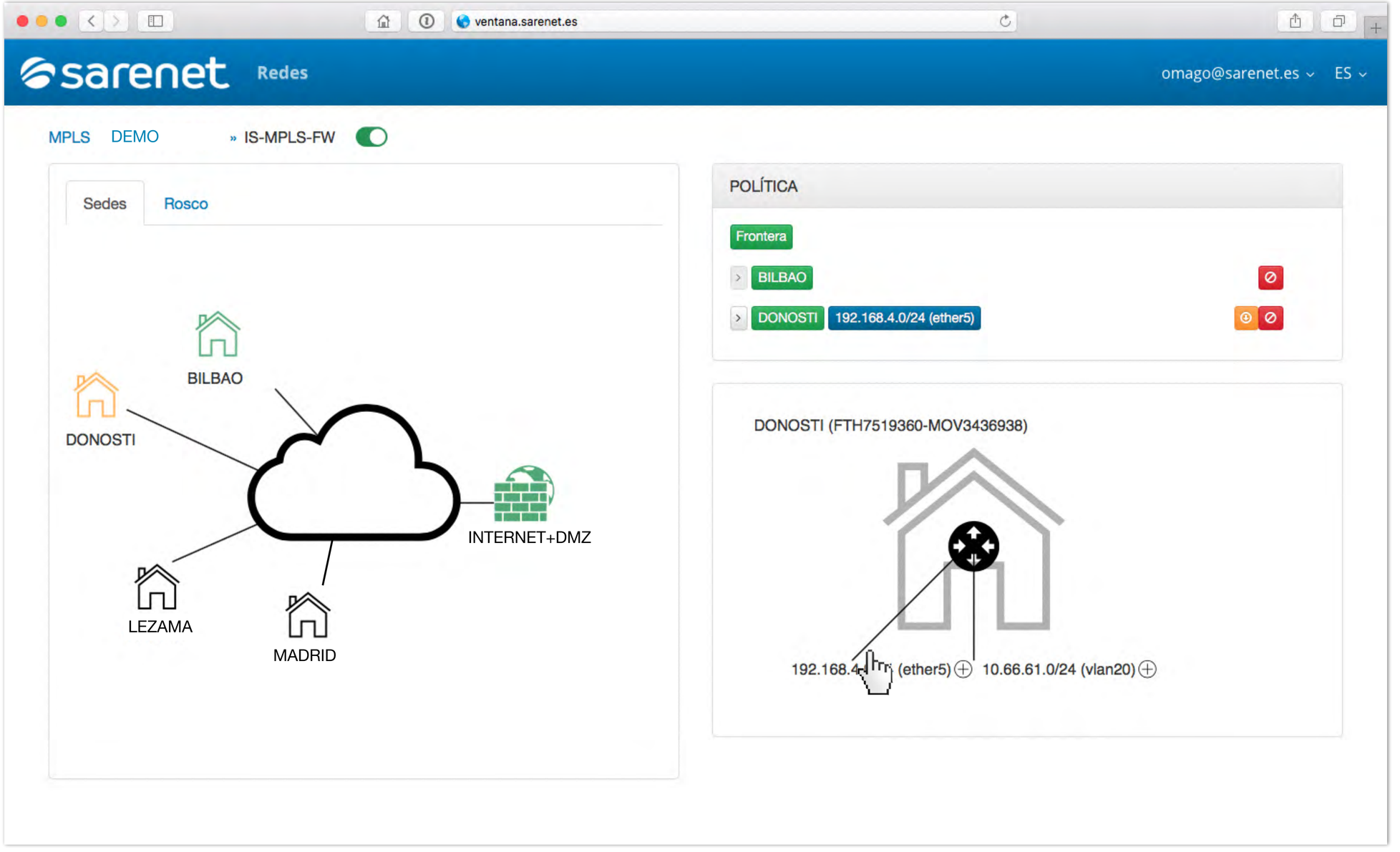
POLÍTICA

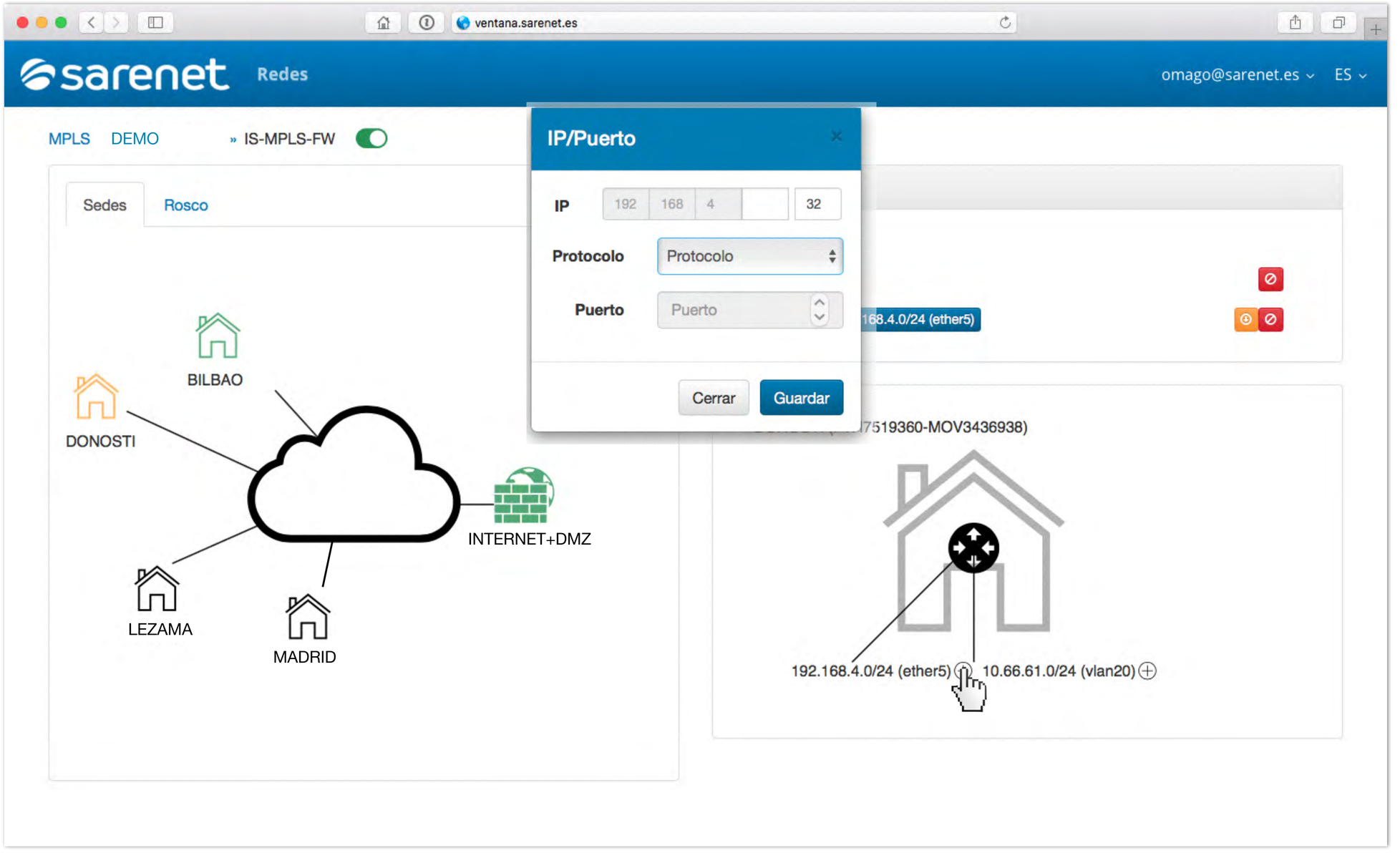
Frontera

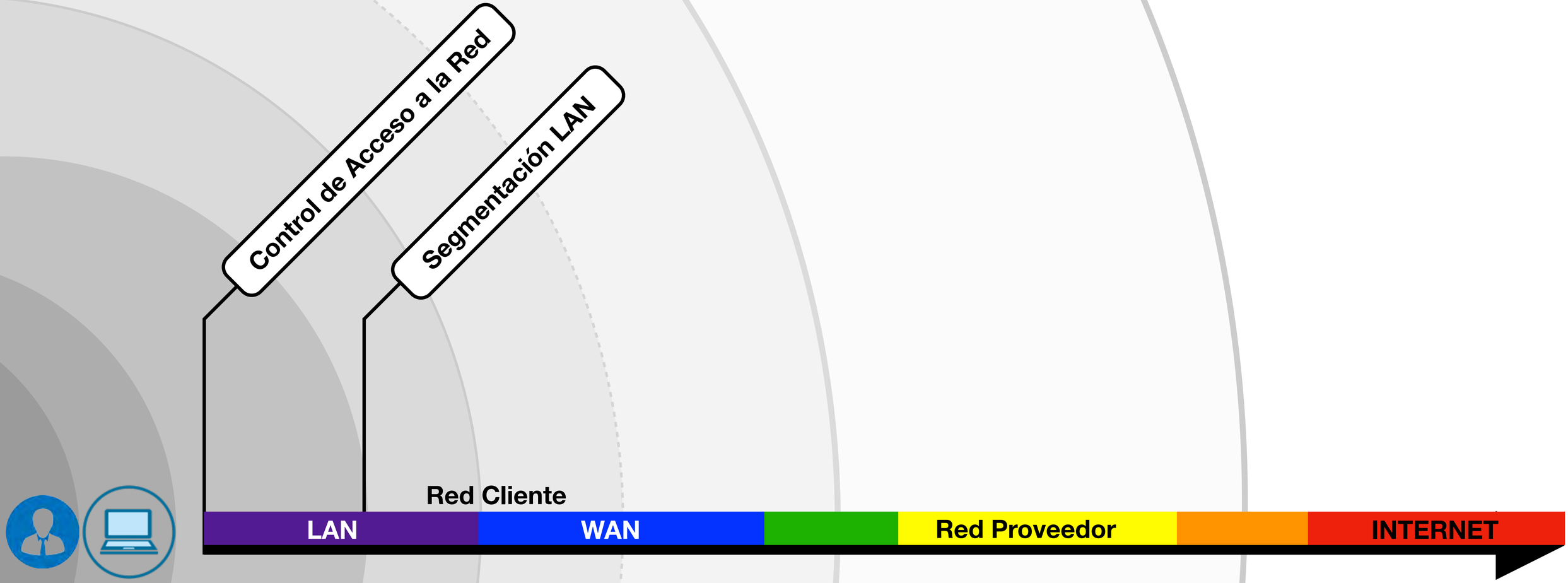
BILBAO

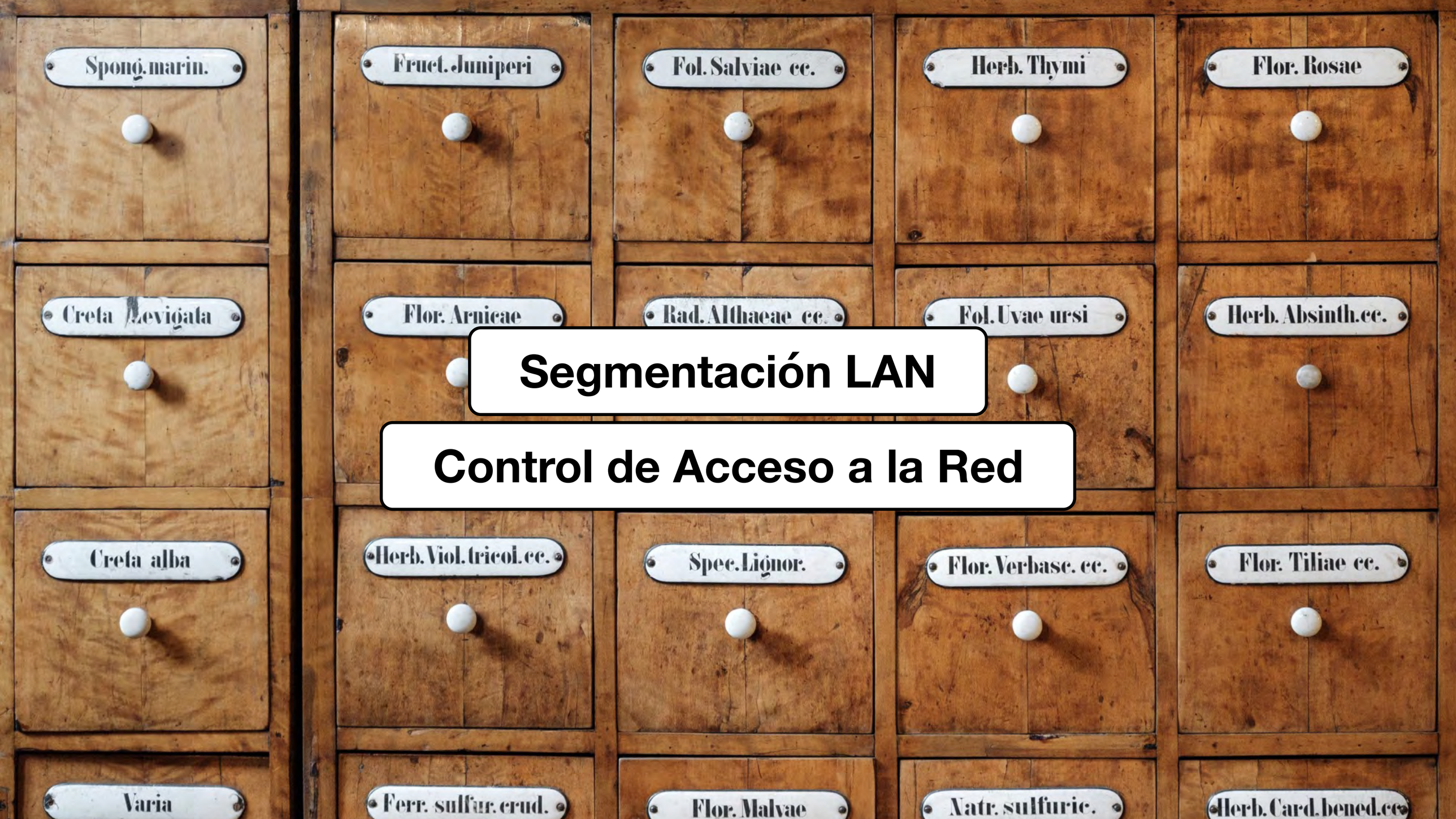
DONOSTI (FTH7519360-MOV3436938)




ventana.sarenet.es
sarenet
Redes
omago@sarenet.es
ES
MPLS
DEMO
» IS-MPLS-FW
Sedes
Rosco
BILBAO
DONOSTI
INTERNET+DMZ
LEZAMA
MADRID
POLÍTICA
Frontera
BILBAO
DONOSTI
192.168.4.0/24 (ether5)
DONOSTI (FTH7519360-MOV3436938)
192.168.4
(ether5)
10.66.61.0/24 (vlan20)

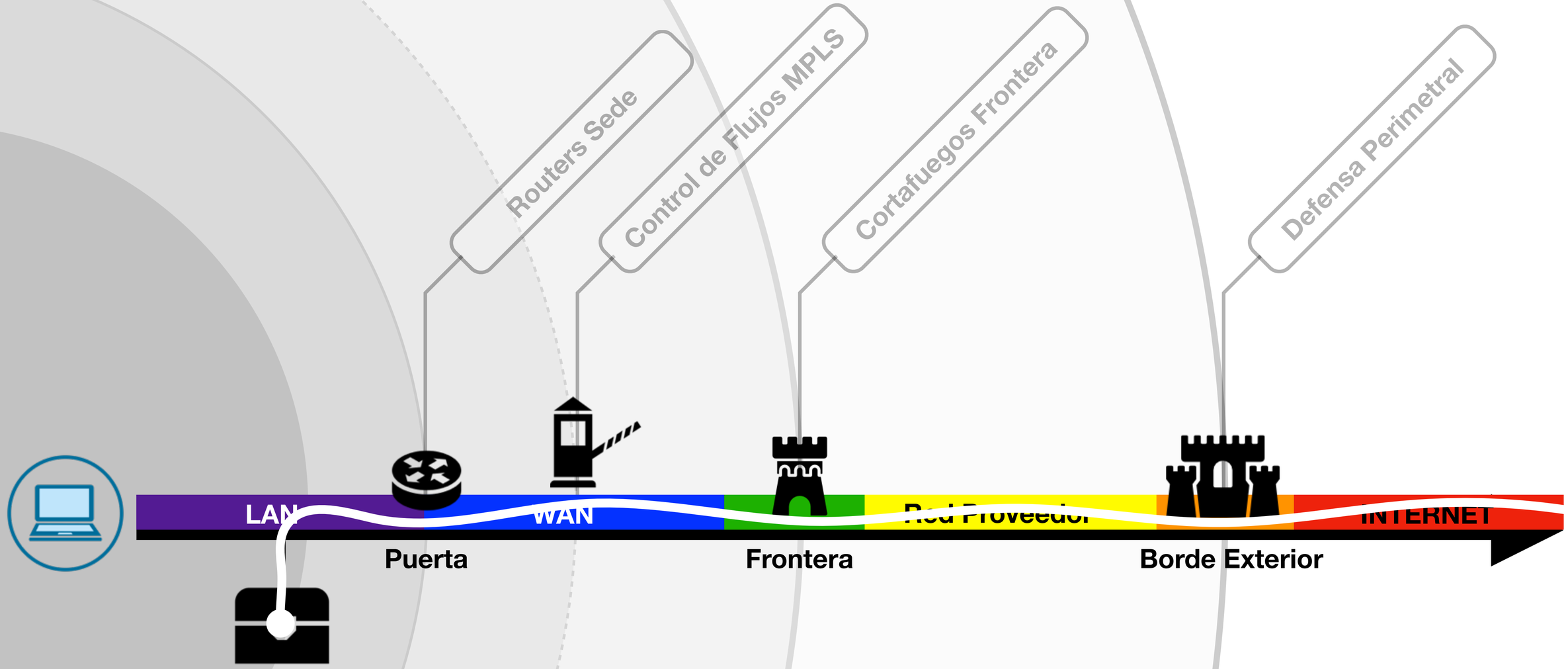

ventana.sarenet.es
sarenet
Redes
omago@sarenet.es
ES
MPLS
DEMO
» IS-MPLS-FW
Sedes
Rosco
IP/Puerto
IP
192
168
4
32
Protocolo
Protocolo
Puerto
Puerto
Cerrar
Guardar
168.4.0/24 (ether5)
BILBAO
DONOSTI
INTERNET+DMZ
LEZAMA
MADRID
7519360-MOV3436938)
192.168.4.0/24 (ether5)
10.66.61.0/24 (vlan20)

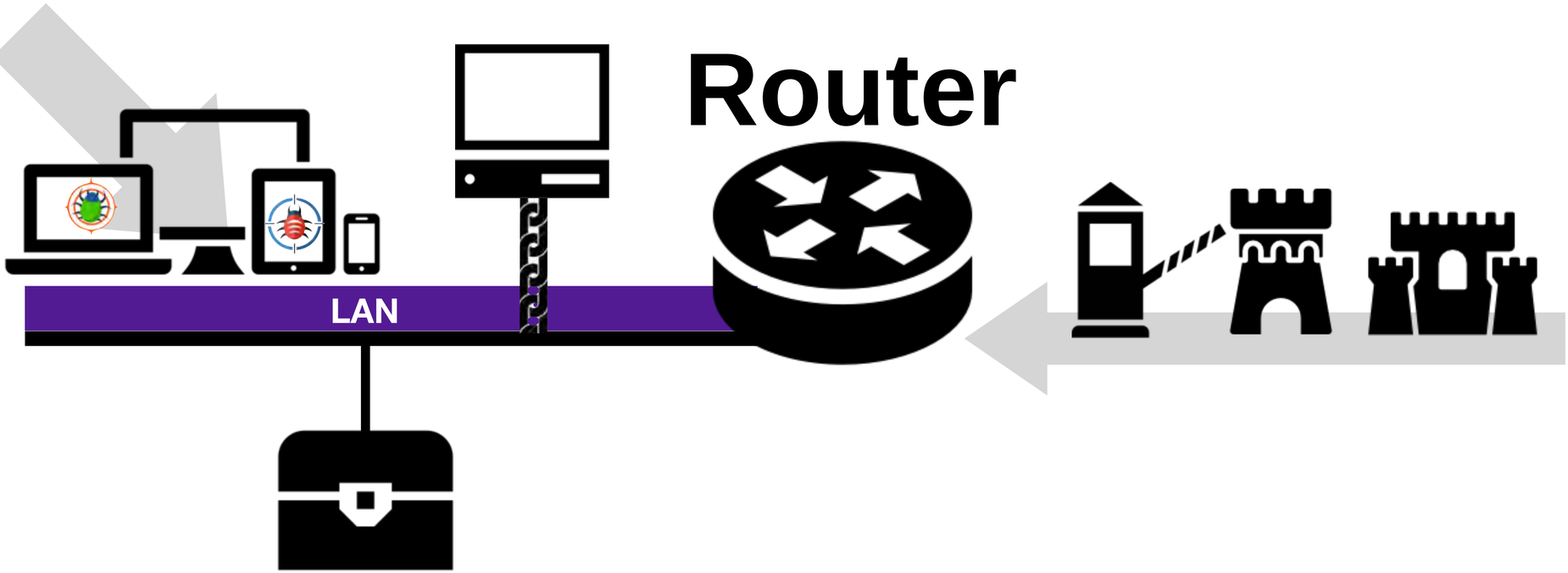

Control de Acceso a la Red
Segmentación LAN
Red Cliente
LAN
WAN
Red Proveedor
INTERNET

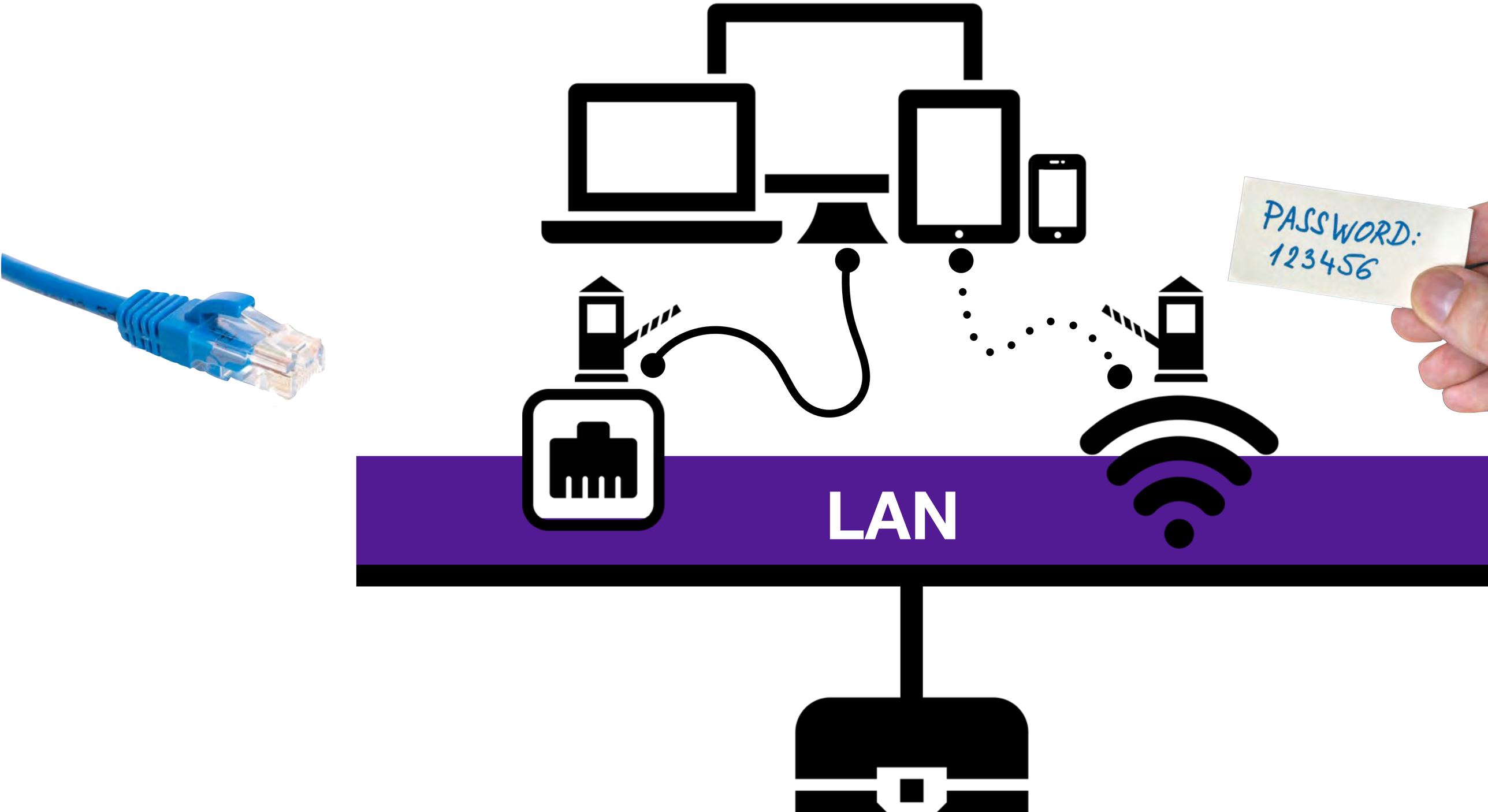


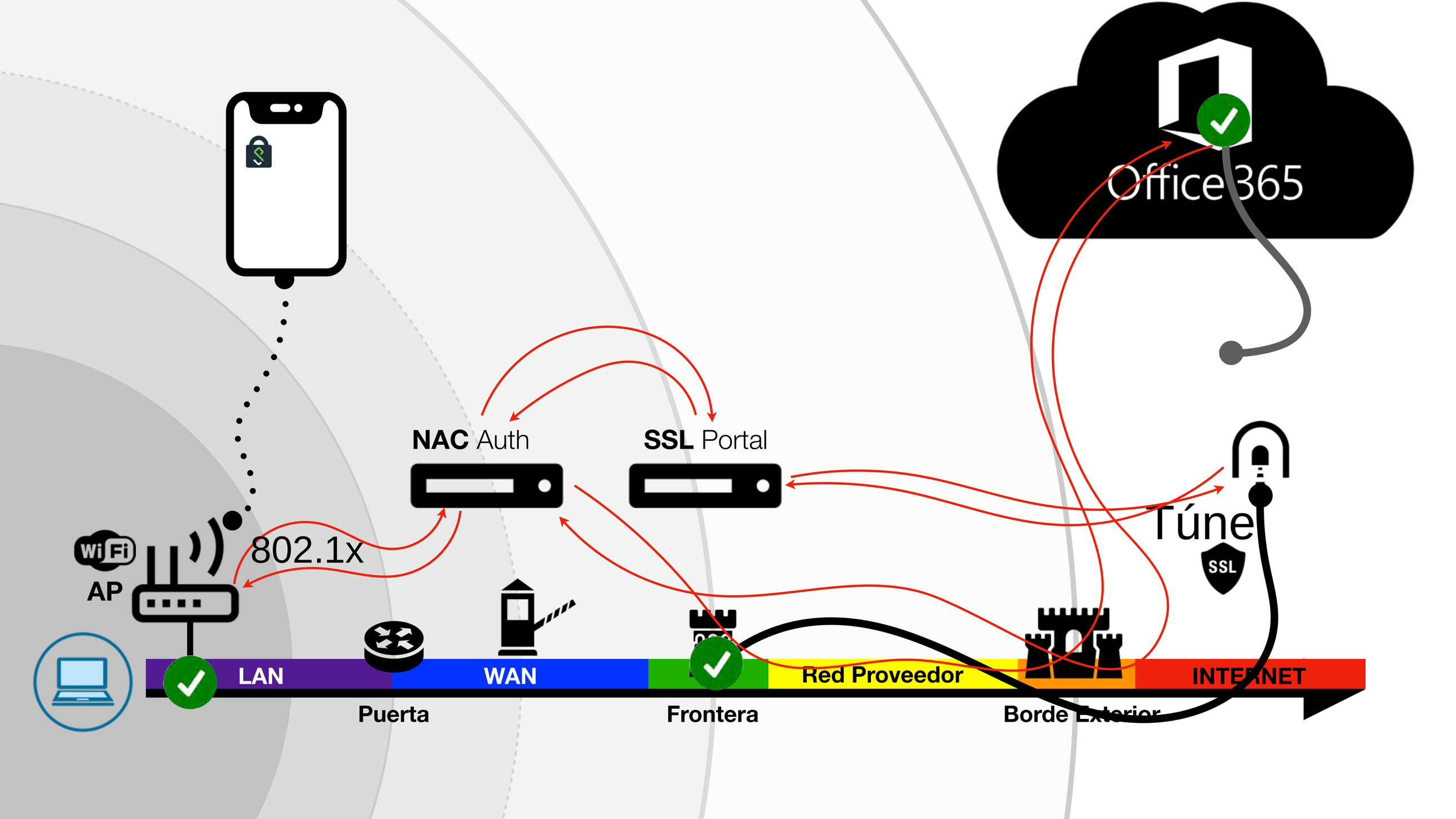
Segmentación LAN

Control de Acceso a la Red


Routers Sede
Control de Flujos MPLS
Cortafuegos Frontera
Defensa Perimetral
LAN
WAN
Red Proveedor
INTERNET
Puerta
Frontera
Borde Exterior


Router
LAN


PASSWORD:
123456
LAN


Office 365
NAC Auth
SSL Portal
802.1x
AP
Túnel
SSL
LAN
WAN
Red Proveedor
INTERNET
Puerta
Frontera
Borde Exterior

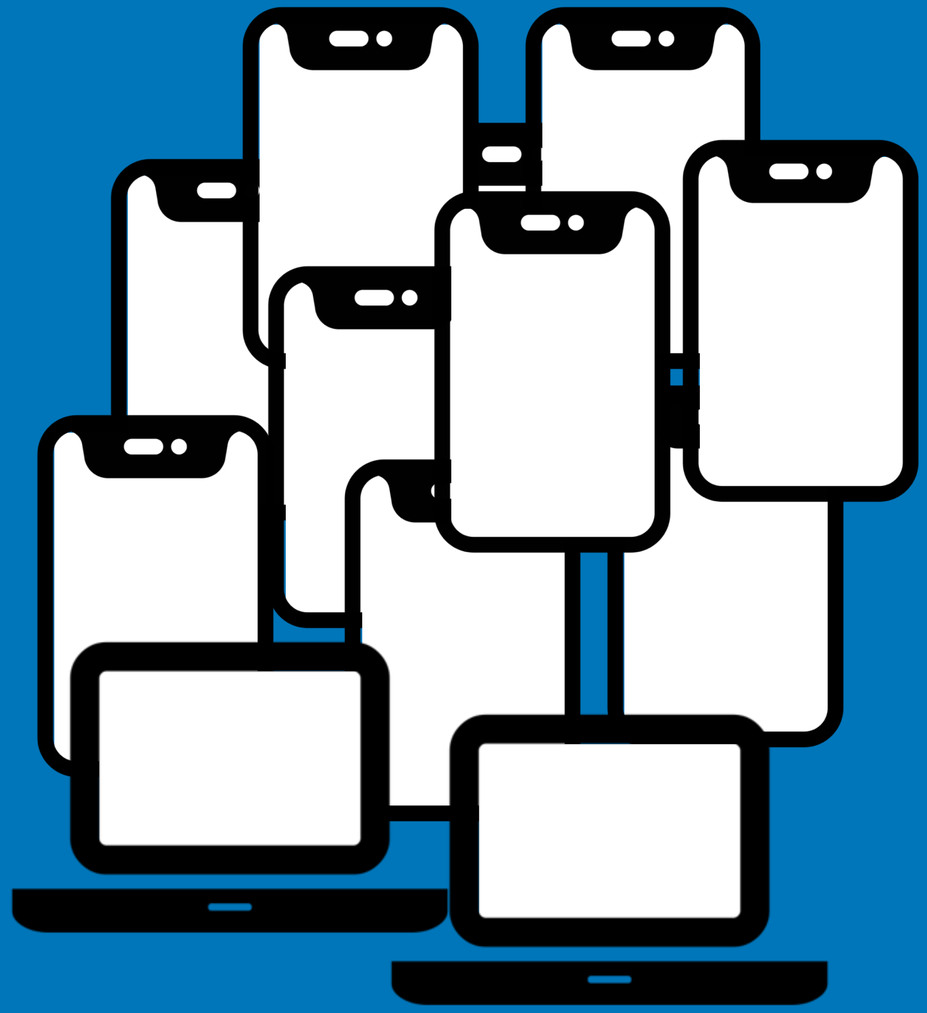
NAC

Control de Acceso a la Red

Invitados

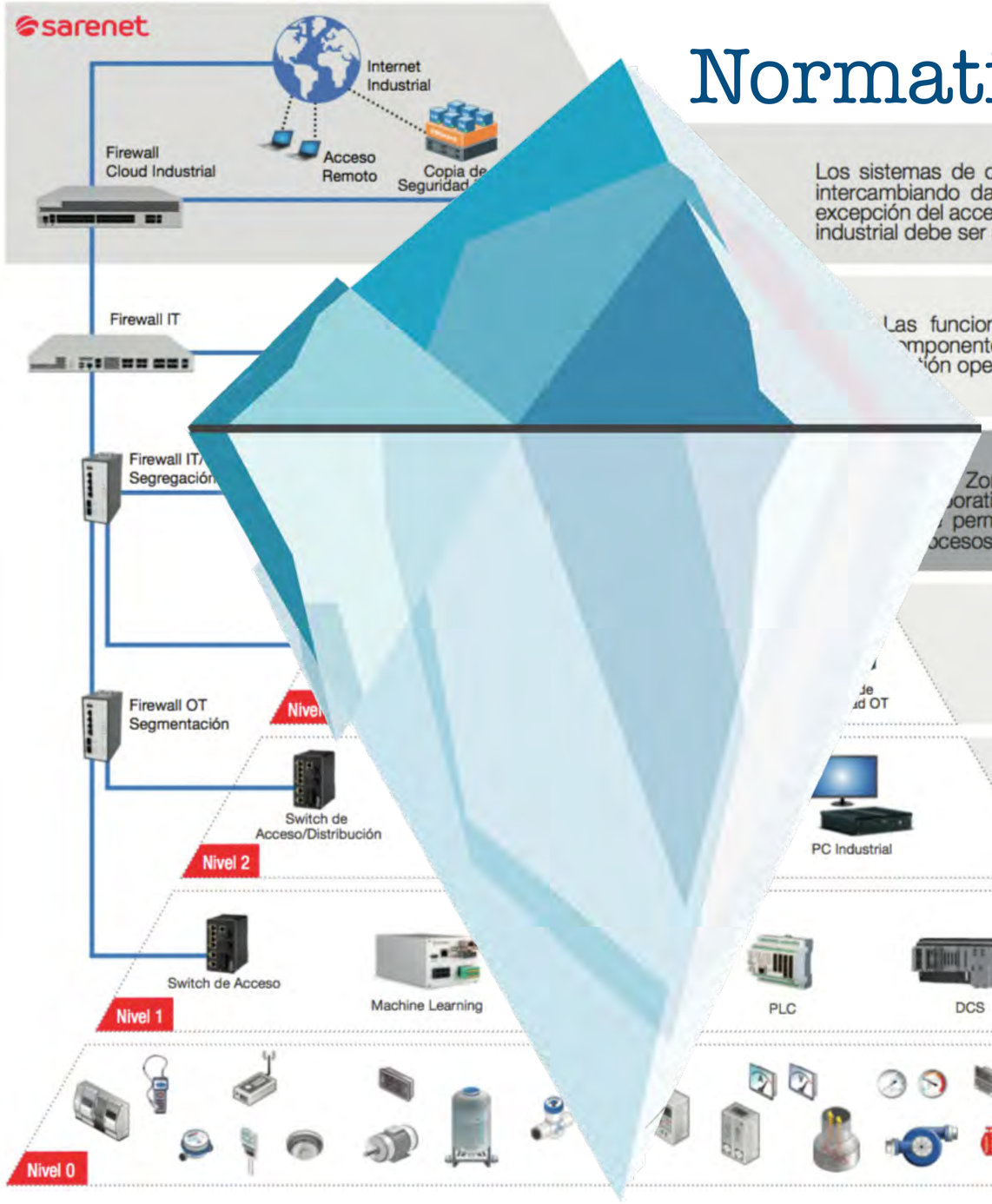
Servicios Críticos

Oficina




Mundo IT
Mundo OT

Normativa **ISA/IEC 62443**



SERVICIOS INTERNET
Los sistemas de control y automatización se integran con las aplicaciones empresariales intercambiando datos de producción. El acceso a éstos no suele ser necesario, con la excepción del acceso de los socios. El acceso a los datos y la red de automatización y control industrial debe ser administrado y controlado para mantener la disponibilidad y la estabilidad.

RED EMPRESA
Las funciones incluyen sistemas financieros empresariales o regionales y otros componentes de infraestructura empresarial, como la programación de producción, la gestión operativa, la gestión de mantenimiento para una planta... Con esta norma, los sistemas de ingeniería también se consideran en este nivel.

IT

ZONA DMZ (Zona Desmilitarizada) IT/OT
Zona que mantiene unos servidores, a los que se accede desde la Red corativa y también desde la Red de Control de Proceso industrial. Es una zona permite obtener datos protegidos desde y hacia el dominio de control de cesos, gestionando el tráfico de datos proveniente del nivel 4 a capas inferiores.

RED OPERACIÓN
Este nivel incluye las funciones involucradas en la gestión de flujos de trabajo para producir los productos finales deseados. Los ejemplos incluyen el envío de producción, la programación detallada de la producción, la fiabilidad y la optimización del control en todo el sitio.

RED SUPERVISIÓN
Este nivel incluye las funciones involucradas en el monitoreo, supervisión y control del proceso físico. Hay múltiples áreas de producción en una planta como destilación, conversión, mezclado, instalaciones de procesamiento...

RED CONTROL
Incluye la detección y manipulación del proceso físico. Lee los datos de los sensores, ejecuta algoritmos y mantiene el historial de procesos. incluye control continuo, control de secuencia, control de lotes y control discreto.

INSTRUMENTACIÓN
Es el nivel de proceso físico real que incluye los sensores y actuadores conectados directamente al proceso y al equipo de proceso.

OT

NAC

Control de Acceso a la Red

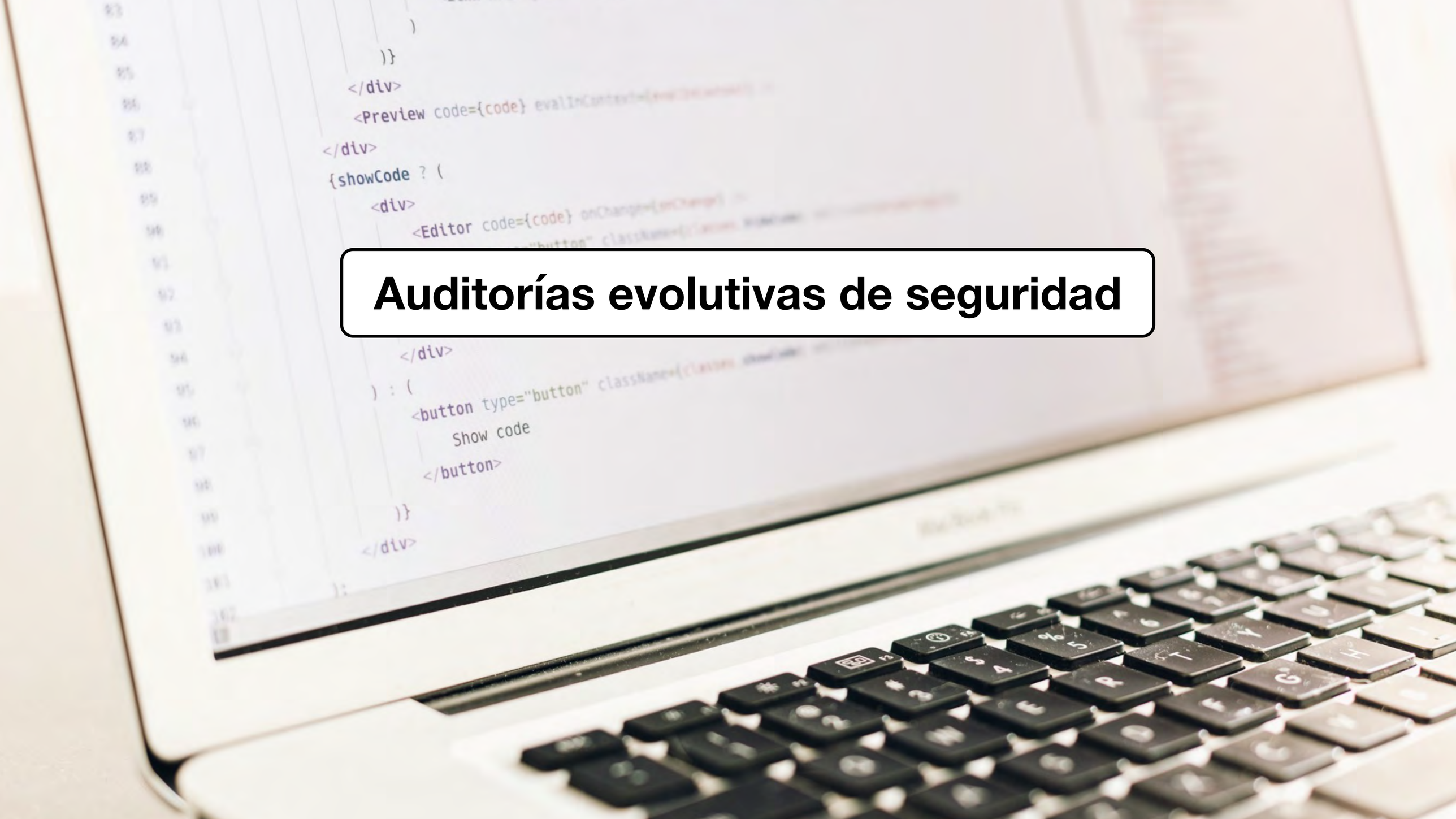
iT/oT

Segmentación LAN

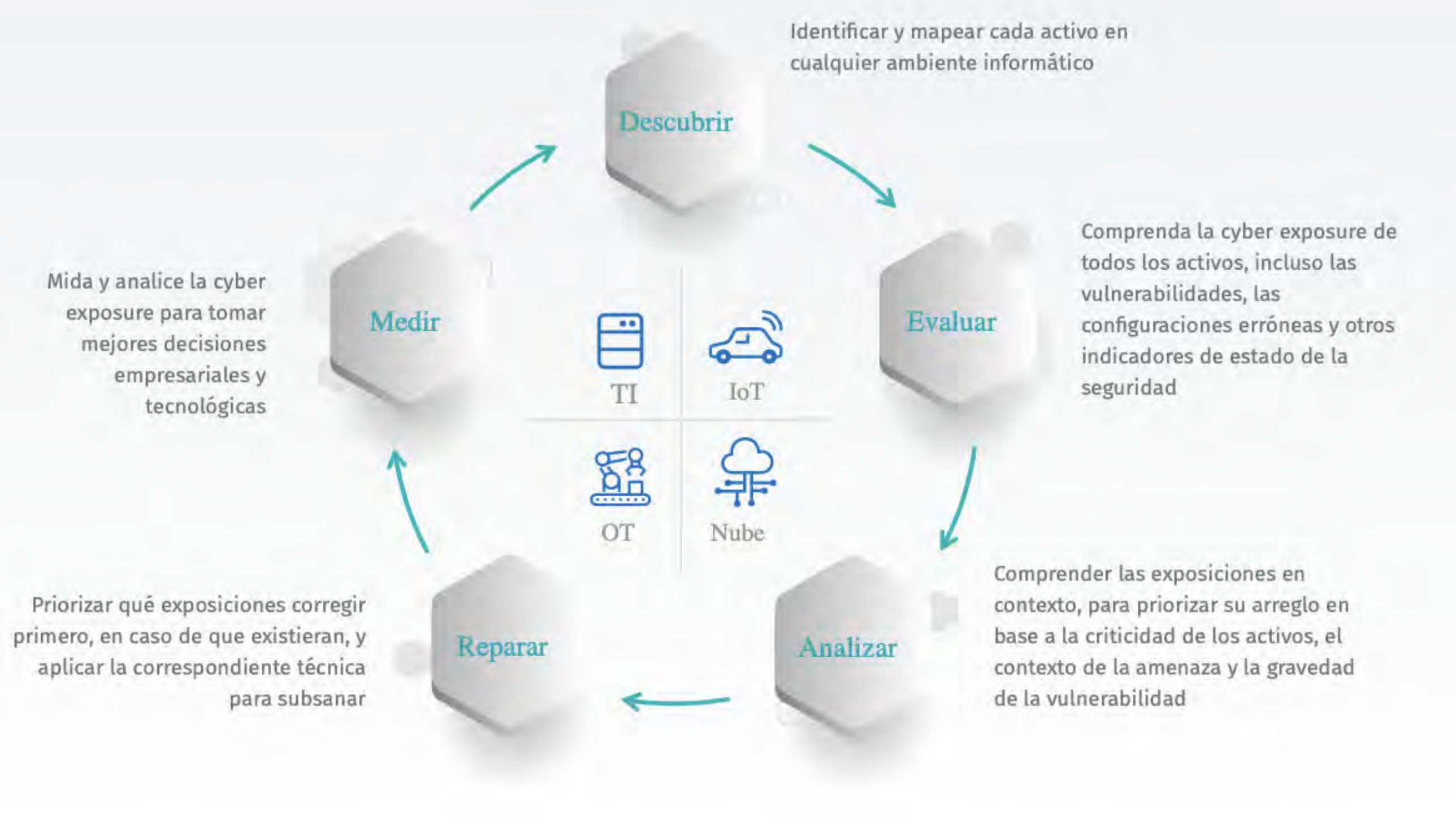

CISCO
IE 2000
EX4200
Pulse Secure
PSA7000
FORTINET
FortiGate 100E
UniFi


sarenet
Control de Acceso a la Red
Segmentación LAN


Red Cliente
LAN
WAN
Red Proveedor
INTERNET
Auditorías evolutivas de Seguridad


Auditorías evolutivas de seguridad


Internet de las cosas
Sistema de control industrial
IoT empresarial
Nube
Infraestructura de la nube
Aplicación web
Contenedor
Dispositivos móviles
Computadoras portátiles y de escritorio
TI
Servidor
Infraestructura de la red


Descubrir
Identificar y mapear cada activo en cualquier ambiente informático
Evaluar
Comprenda la cyber exposure de todos los activos, incluso las vulnerabilidades, las configuraciones erróneas y otros indicadores de estado de la seguridad
Analizar
Comprender las exposiciones en contexto, para priorizar su arreglo en base a la criticidad de los activos, el contexto de la amenaza y la gravedad de la vulnerabilidad
Reparar
Priorizar qué exposiciones corregir primero, en caso de que existieran, y aplicar la correspondiente técnica para subsanar
Medir
Mida y analice la cyber exposure para tomar mejores decisiones empresariales y tecnológicas
TI
IoT
OT
Nube

tenable.sc™

Identifique, investigue y priorice vulnerabilidades de forma precisa.

Cada organización, sin importar su tamaño, podrá responder con certeza las preguntas siguientes:

1. *¿Dónde estamos expuestos?*
2. *¿Dónde debemos dar prioridad en función del riesgo?*
3. *¿Estamos reduciendo la exposición con el tiempo?*
4. *¿Qué resultado obtenemos si nos comparamos con nuestros pares?*

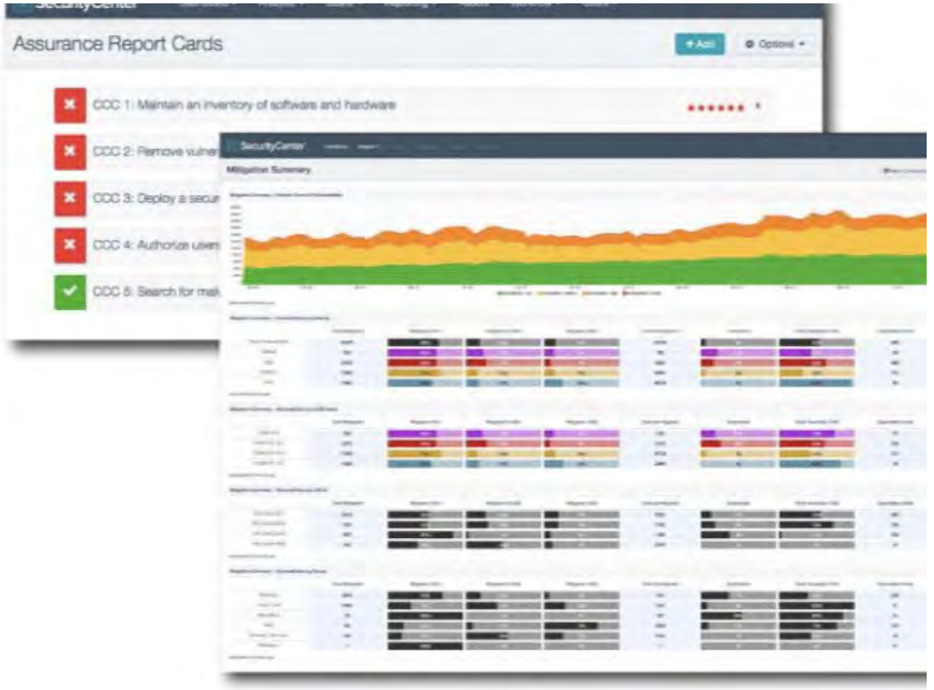
tenable

sarenet

tenable.sc™

Identifique, investigue y priorice vulnerabilidades de forma precisa.

Capacidades	
Gestión de vulnerabilidades centralizada con múltiples escáneres	✓
Clasificación dinámica de activos (servidor de correo, servidor web, etc.)	✓
Auditoría de configuración basada en políticas	✓
Detección de malware con inteligencia de amenazas integrada	✓
Paneles/informes predefinidos con alimentación automática de Tenable	✓
Respuesta ante incidentes con alertas, notificaciones y tickets configurables	✓
Assurance Report Cards (ARC)	✓



Tenable.sc proporciona análisis de vulnerabilidades, tendenci informes y flujos de trabajo altamente personalizables para adaptarse a las necesidades de su programa de seguridad

tenable

sarenet

tenable.sc™

Identifique, investigue y priorice
vulnerabilidades de forma precisa.

Common Vulnerability Scoring System

CVSS es un sistema de puntuación que proporciona **un método estándar y abierto para estimar el impacto de una vulnerabilidad** y que se compone tres grupos principales de métricas: Base, Temporal y de Entorno (Environmental). Cada uno de estos grupos se compone a su vez de un conjunto de métricas.

Grupo Base: Engloba las cualidades intrínsecas de una vulnerabilidad y que son independientes del tiempo y el entorno. Las métricas evaluadas en este grupo son:

- **Access Vector (AV)**. Valores: [L,A,N] (Local, Adjacent, Network
- **Access Complexity (AC)**. Valores [H,M,L] (High, Medium, Low)
- **Authentication (Au)**. Valores [M,S,N] (Multiple, Single, None)
- **Confidenciality Impact (C)** . Valores [N,P,C] (None, Partial, Complete)
- **Integrity Impact (I)**. Valores [N,P,C] (None, Partial, Complete)
- **Availability Impact (A).** Valores [N,P,C] (None, Partial, Complete)

Grupo Temporal: Características de la vulnerabilidad que cambian en el tiempo. Se aplican tres métricas::

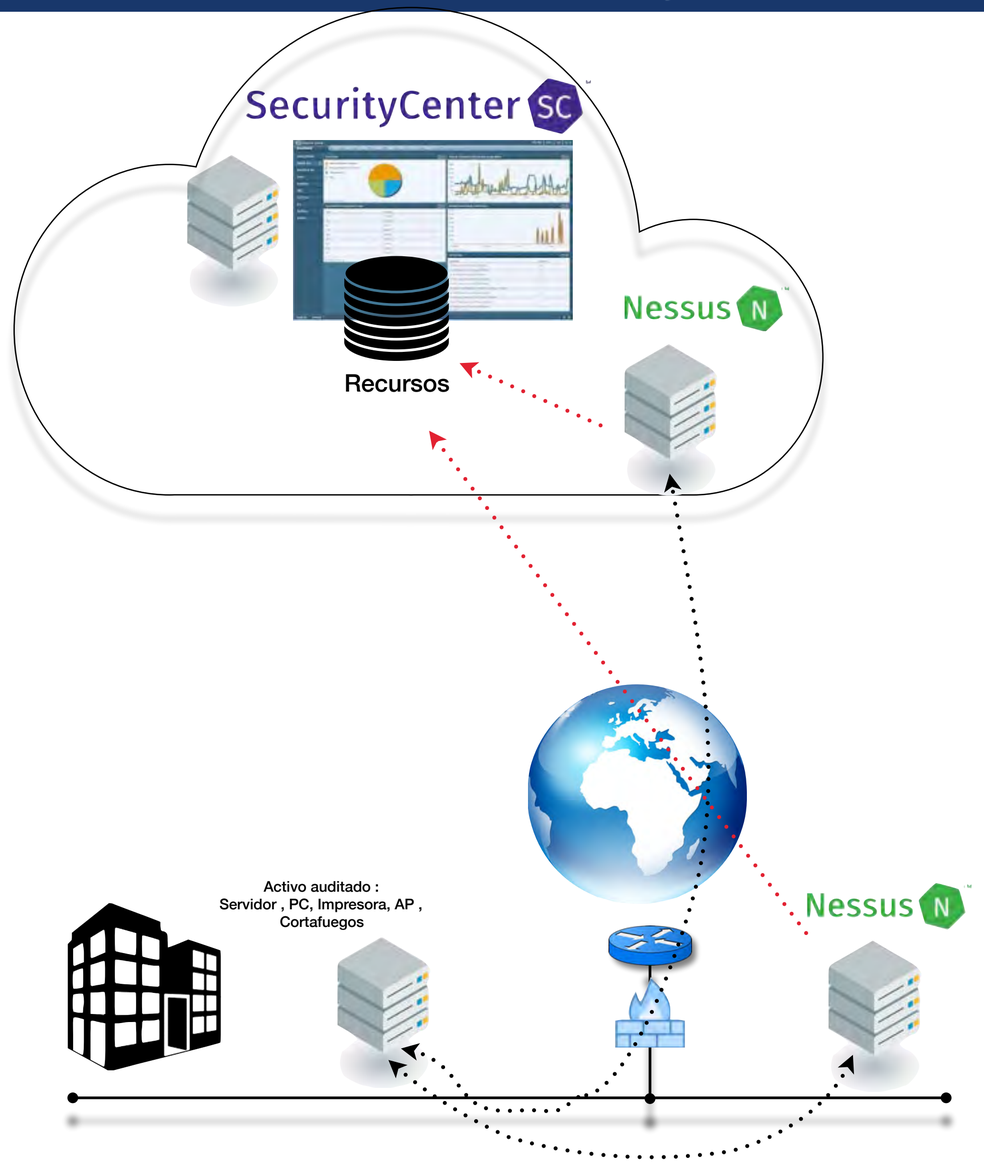
- **Exploitability (E).** Valores: [U,POC,F,H,ND] (Unproven, Proof-of-Concept, Functional Exploit, High, Not Defined)
- **Remediation Level (RL).** Valores: [OF,TF,W,U,ND] (Official Fix, Temporary Fix, Workaround, Unavailable, Not Defined)
- **Report Confidence (RC).** Valores: [UC,UR,C,ND] (Unconfirmed, Uncorroborated, Confirmed, Not Defined)

Grupo Environmental: Las características de la vulnerabilidad relacionadas con el entorno del usuario. En este caso los factores que se evalúan son:

- **Collateral Damage Potential (CDP).** Valores: [N,L,LM,MH,H,ND] (None, Low, Low Medium, Medium High, High, Not Defined)
- **Target Distribution (TD).** Valores: :[N,L,M,H,ND] (None, Low, Medium, High, Not Defined)
- **Security Requirements (CR, IR, AR).** Valores: [L,M,H,ND] (Low, Medium, High, Not Defined)

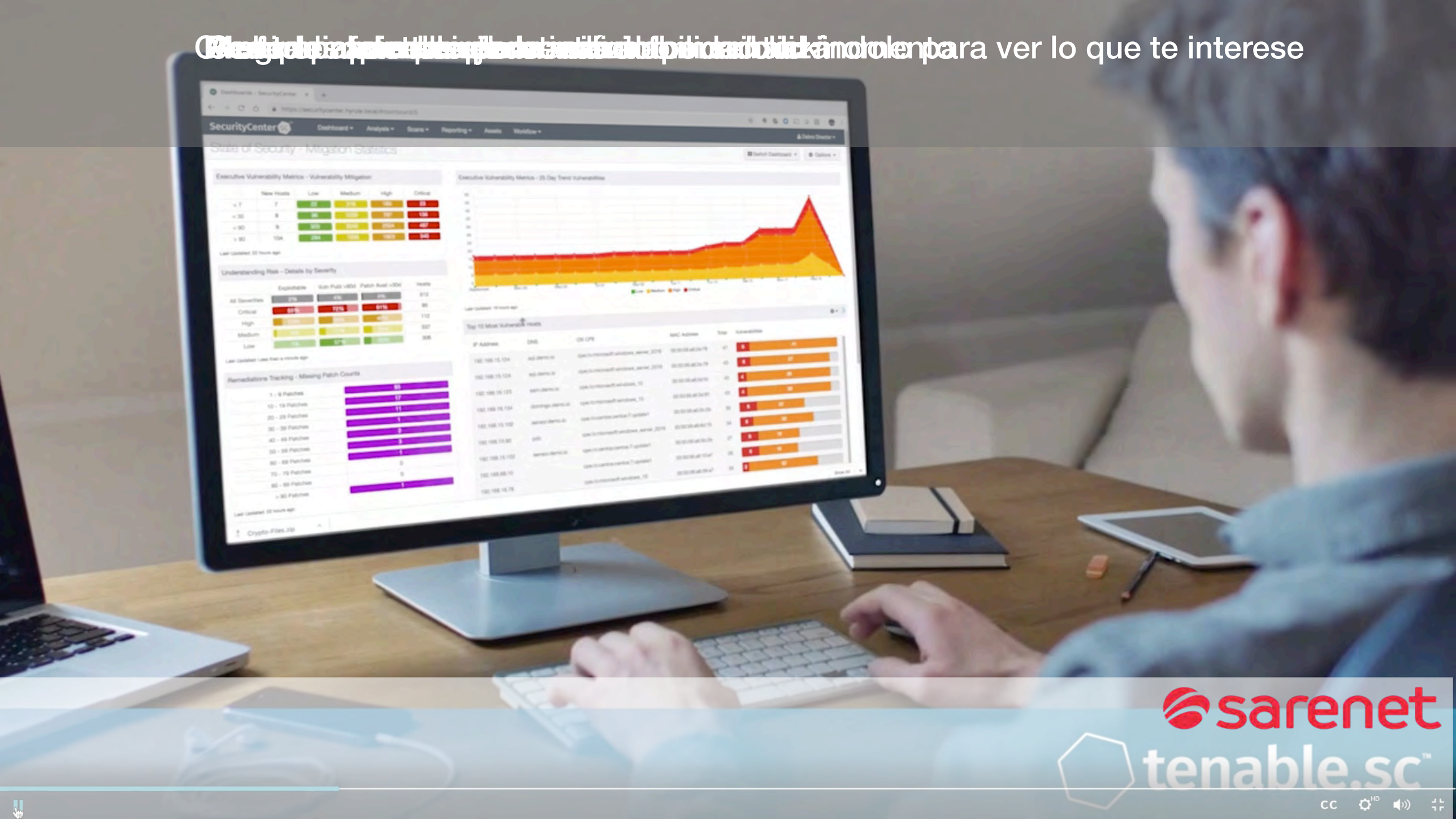
tenable.sc™

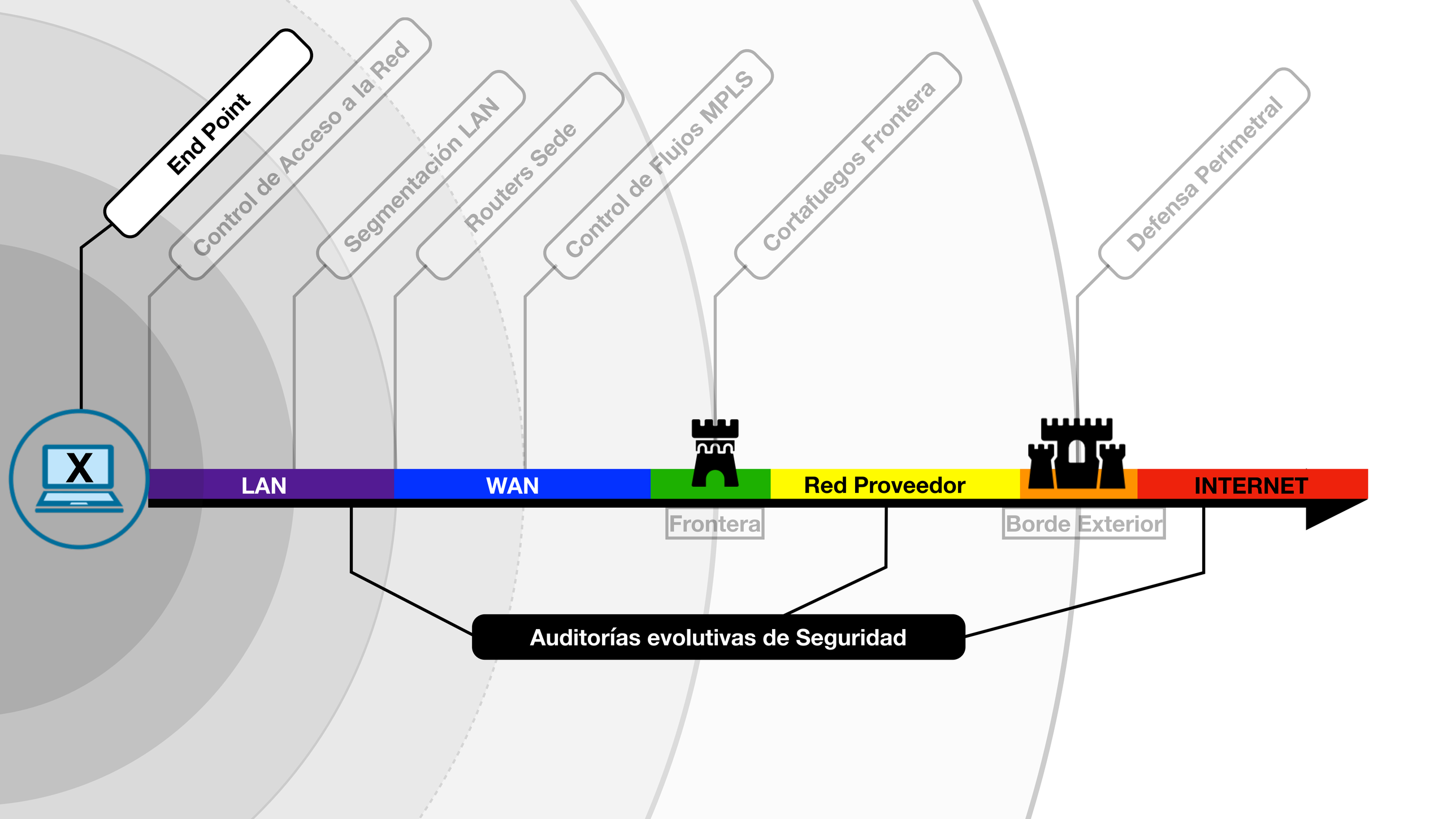
Identifique, investigue y priorice vulnerabilidades de forma precisa.

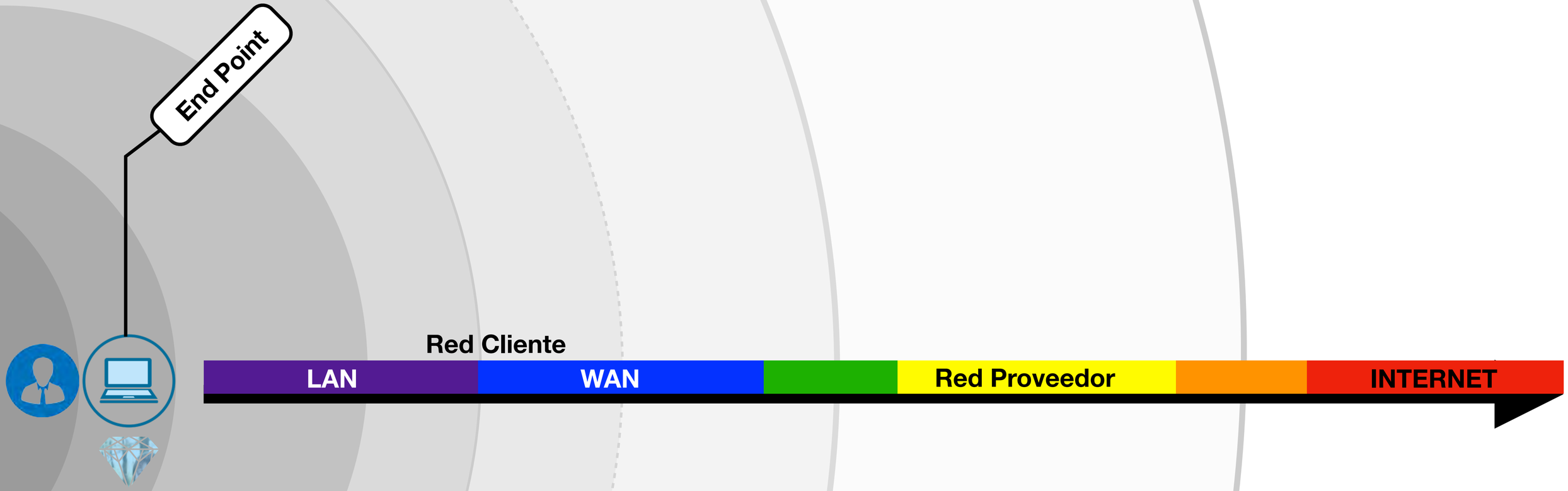


tenable

sarenet


SecurityCenter
Dashboard
Analysis
Scans
Reporting
Assets
Workflow
Executive Vulnerability Metrics - Vulnerability Mitigation
Executive Vulnerability Metrics - 25 Day Trend Vulnerabilities
Understanding Risk - Details by Severity
Remediations Tracking - Missing Patch Counts
Top 10 Most Vulnerable Hosts
sarenet
tenable.sc™


End Point
Control de Acceso a la Red
Segmentación LAN
Routers Sede
Control de Flujos MPLS
Cortafuegos Frontera
Defensa Perimetral
X
LAN
WAN
Red Proveedor
INTERNET
Frontera
Borde Exterior
Auditorías evolutivas de Seguridad


End Point
Red Cliente
LAN
WAN
Red Proveedor
INTERNET


Enter
End Point

Historia de Sophos

Evolución hacia la protección completa

Hito

1985

Founded in Abingdon (Oxford), UK

Peter Lammer c1985

Jan Hruska c1985

1988

First checksum-based antivirus software

Inicio

1989

First signature-based antivirus software

1996

Voted best small/ medium sized company in UK

US presence established in Boston

2003

Acquired ActiveState

ActiveState
Code to Cloud: Smarter, Safer, Faster

Acquired Utimaco Safeware AG

utimaco safeware

SafeGuard Enterprise Encryption

Acquired Astaro

astaro internet security

Acquired DIALOGS

DIALOGS connecting business

Divested non-core Cyber business

Acquired Cyberoam

Cyberoam

Acquired Mojave Networks

mojave

IPO London Stock Exchange

London Stock Exchange

Sophos XG

IPS +40% Optimized IPS Engine
Firewall +50% FastPath Optimization
Anti-Virus +250% Improved Proxy Architecture

2015

Acquired Reflexion

Reflexion

Launched Synchronized Security with Security Heartbeat

Acquired Surfright

SurfRight

Acquired Invincea

invincea

INTERCEPT X

SOPHOS

Acquired PhishThreat

Acquired Barricade

SOPHOS

sarenet

400,000

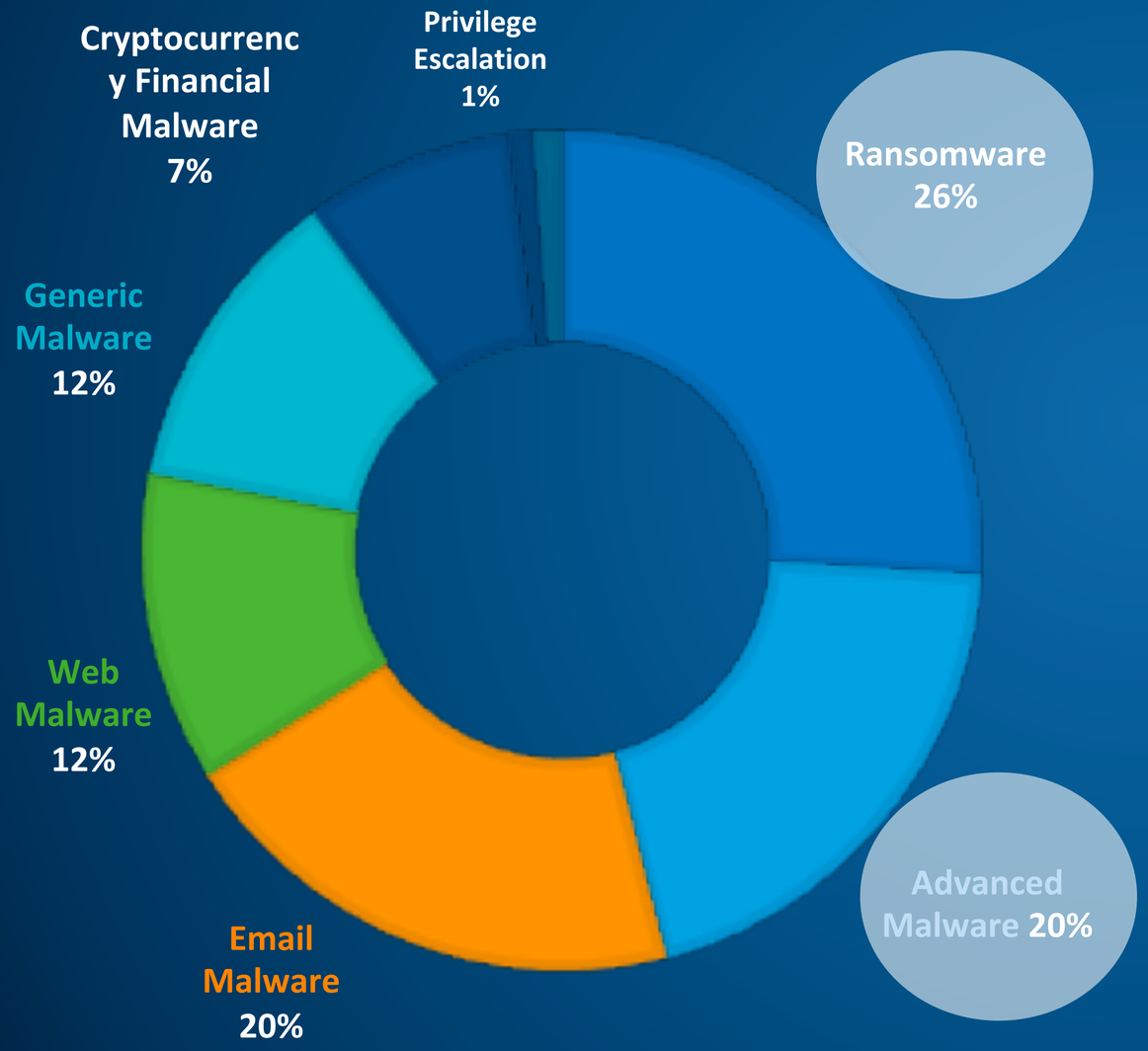
SophosLabs receives and processes 400,000 previously unseen malware samples each day.

75% of the malicious files SophosLabs detects are found only within a single organization.

SOPHOS

Source: SophosLabs

EL PANORAMA DE LAS AMENAZAS HA EVOLUCIONADO



Ransomware

54% de las organizaciones ha sufrido ramsomware al menos 2 veces en 2017^

Advanced Threats

83% está de acuerdo en que es muy difícil detener estas amenazas^

Exploits

La mayor parte de las empresas no cuenta con protección contra exploits^

SOPHOS

Source: SophosLabs

^Source: The State of Endpoint Security Today Survey

sarenet

Yo lo compraría sólo por el nombre .....

Ransomware - Wannacry (ficheros)
Petya - MBR (registro de arranque maestro)

Gartner®

“Leader”

2018 Endpoint Protection Platform Magic Quadrant
Leader in all ten reports since it was first published
One of only 3 leaders

Winner
Security Innovation
of the Year

FORRESTER®

“Leader”

The Forrester Wave: Endpoint Security Suites
Off the charts strategy rating

Winner
Innovation Award
Endpoint Security

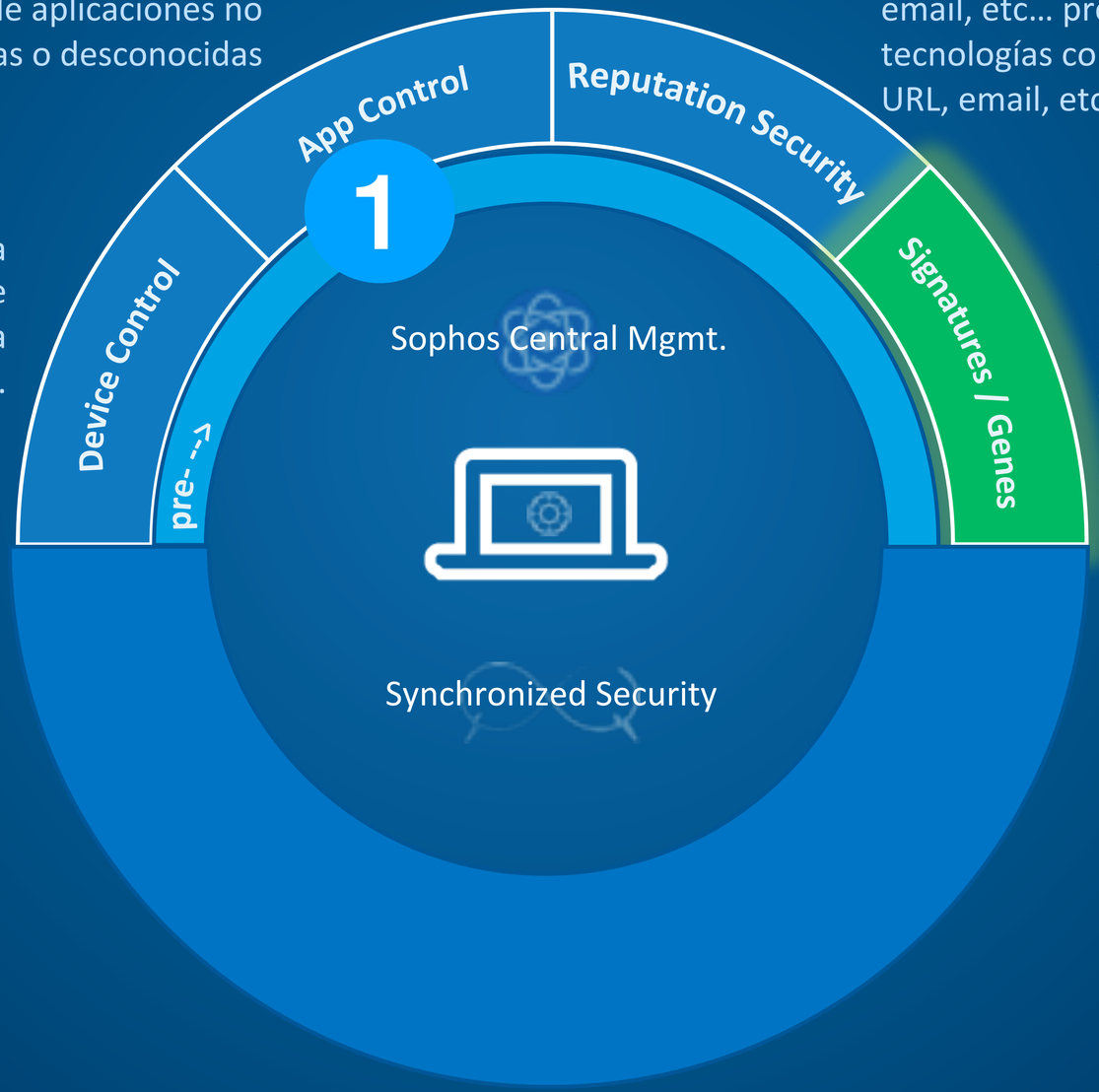
Protección Endpoint Tradicional

Para servidores o puestos, App Control previene de la ejecución de aplicaciones no deseadas o desconocidas

Conociendo el origen/reputación de un fichero, URL, email, etc… previene ataques antes que sucedan. Incluye tecnologías como MTD, reputación de descarga, filtrado URL, email, etc…

Control de políticas para dispositivos extraíbles para que éstos no pongan en riesgo la corporación.

Detección de scripts, macros, documentos y malware como primera línea eficiente de defensa contra variantes conocidas,



- .exe Malware
- Non-.exe Malware
- Script-based Malware
- Phishing Attacks

- Malicious URLs
- Removable Media
- Unauthorized Apps

SOPHOS

sarenet

Gestion Centralizada

1

Control total

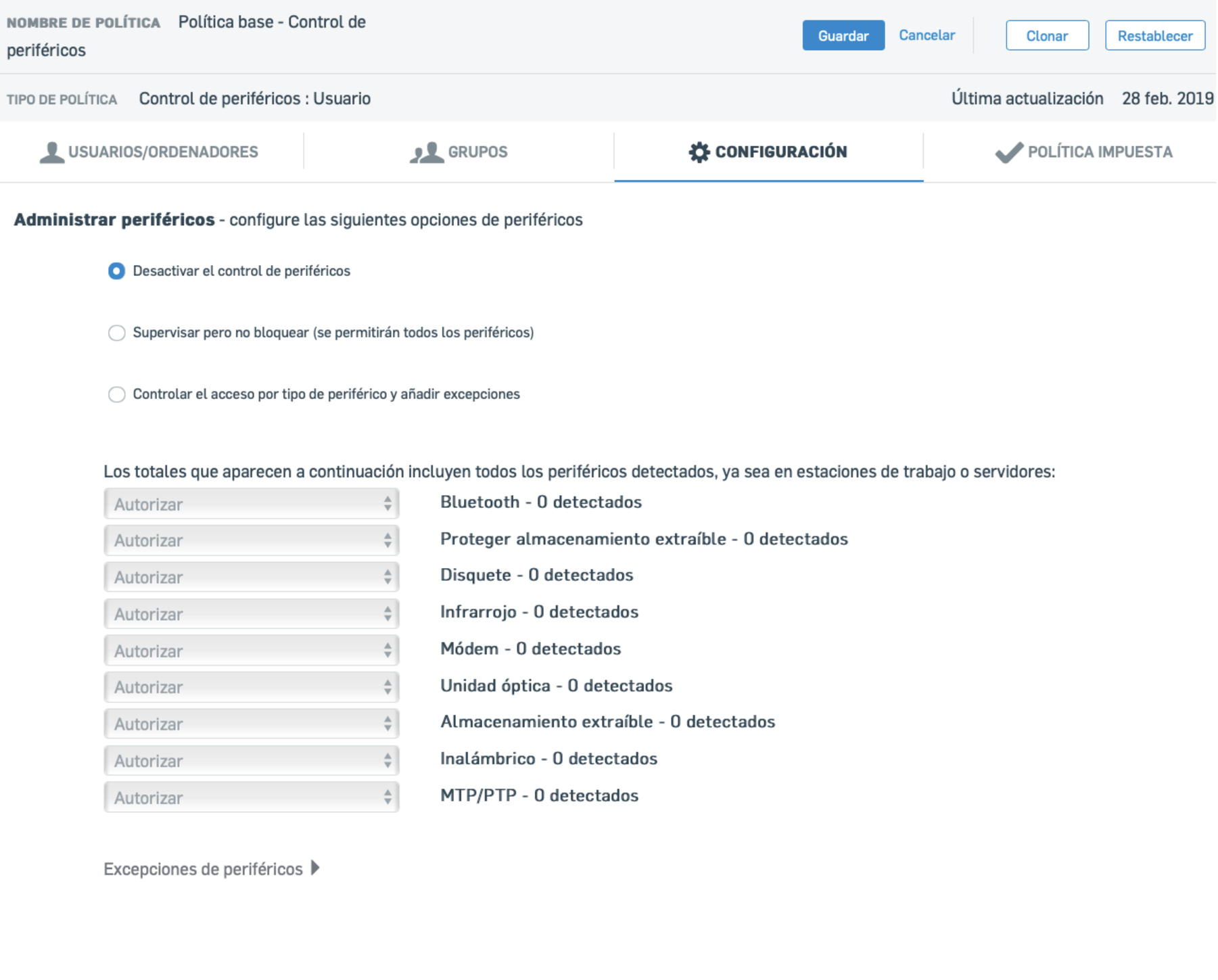
Aplique sus políticas de datos, dispositivo, aplicación y web con facilidad, gracias a la perfecta integración en el agente para estaciones y en la consola de administración.

- **Control web** Filtrado web basado en categorías aplicado dentro y fuera de la red corporativa
- **Control de la aplicación** Bloqueo de aplicaciones por categoría o por nombre con solo un clic
- **Control del dispositivo** Acceso controlado a medios extraíbles y dispositivos móviles
- **Control de datos** Prevención de pérdida de datos (DLP) que utiliza reglas preintegradas o personalizadas

Simplicidad sofisticada

Al igual que su aplicación favorita para web o teléfonos inteligentes, Sophos Endpoint Protection ofrece una funcionalidad sofisticada junto con una experiencia de usuario sencilla e intuitiva.

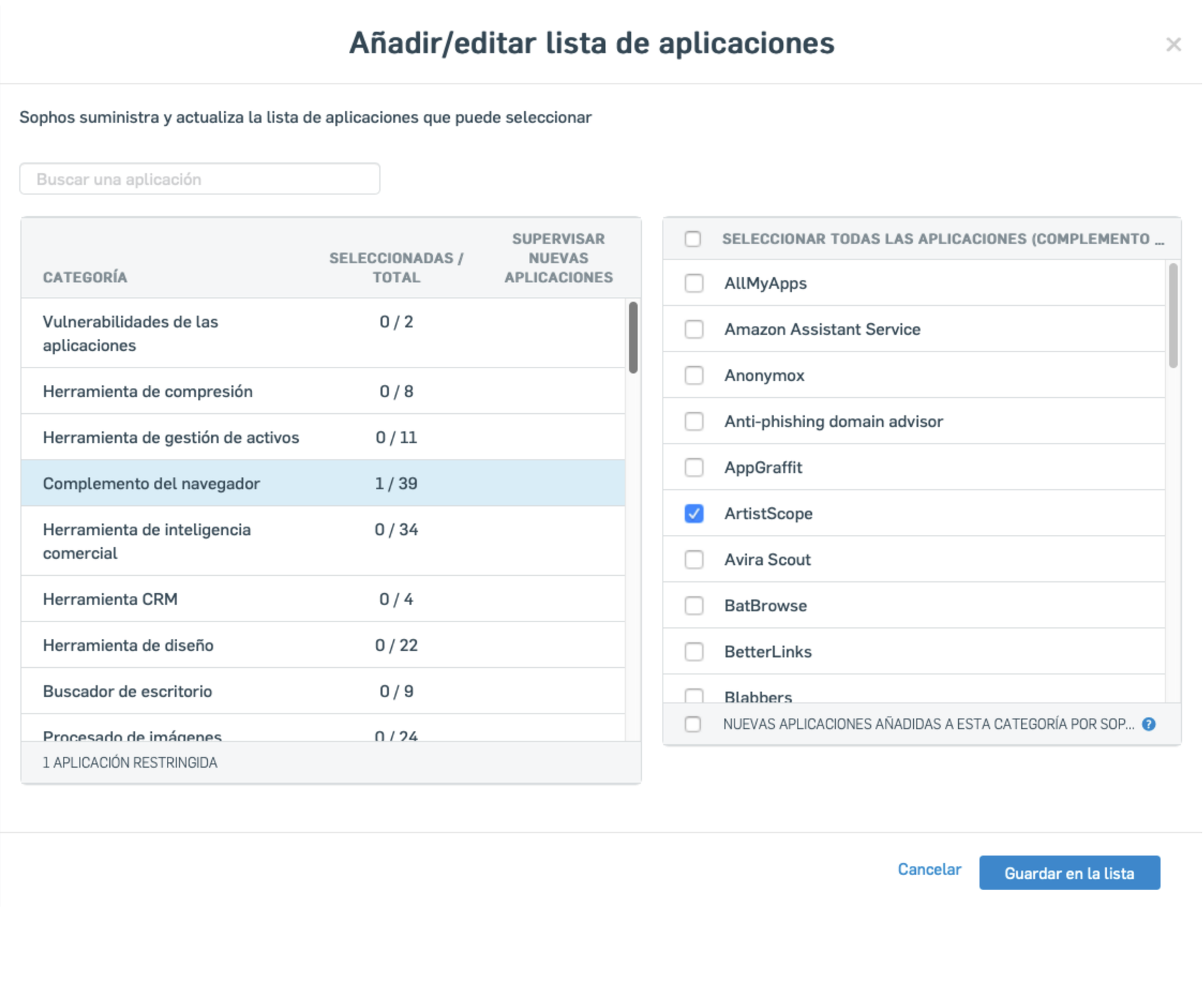
- Despliegue rápido y sencillo desde la nube o de forma local
- Políticas predeterminadas que se configuran para equilibrar la protección, usabilidad y rendimiento
- Eliminación automática de productos de seguridad para estaciones de terceros
- Configuración sencilla de funciones avanzadas tales como HIPS y control de dispositivo, gracias a los datos continuamente actualizados de SophosLabs



1

Por ejemplo, podemos crear una política sobre los periféricos autorizados

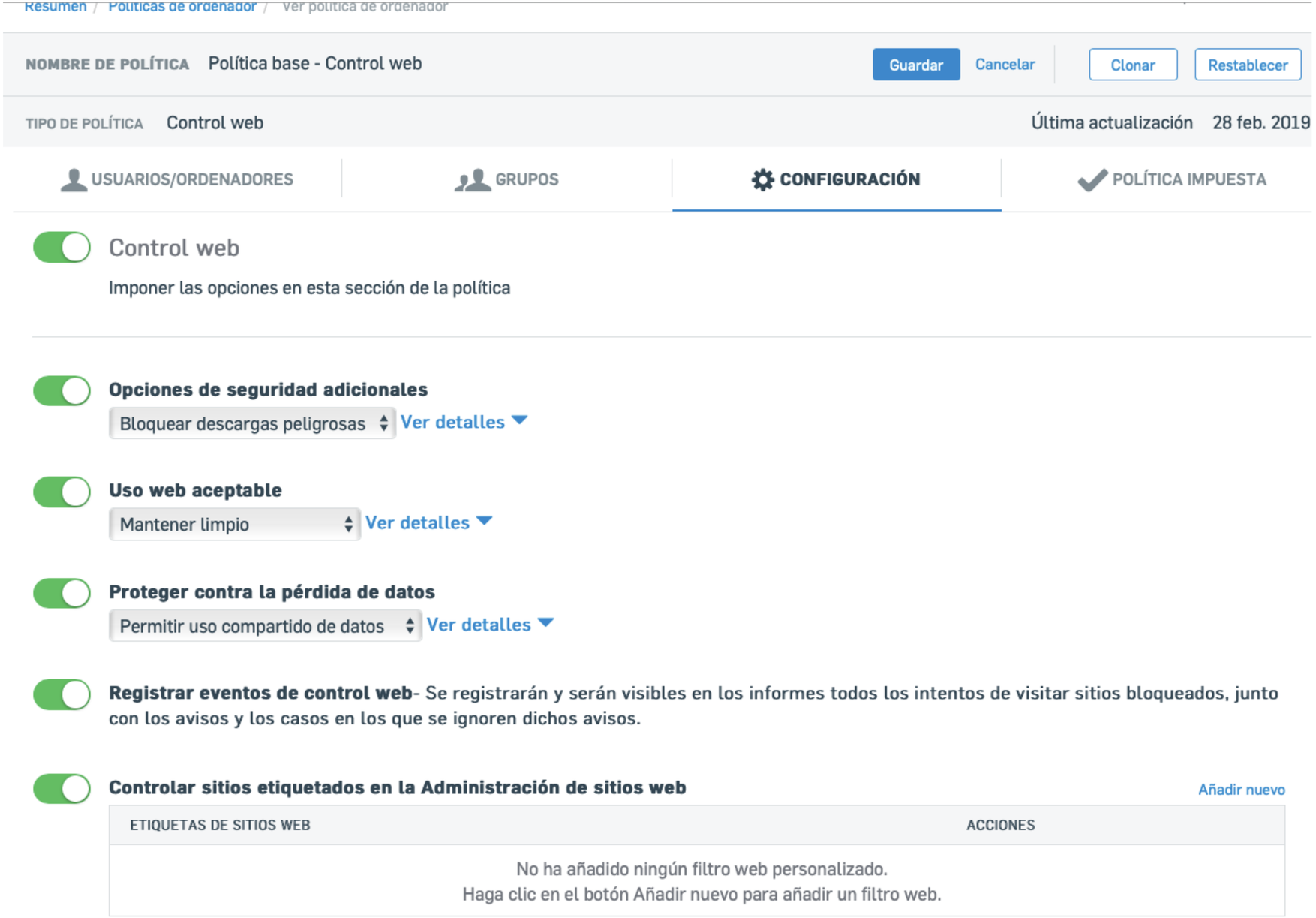
sarenet



1

O … las aplicaciones que dejamos , o no , utilizar

sarenet



1

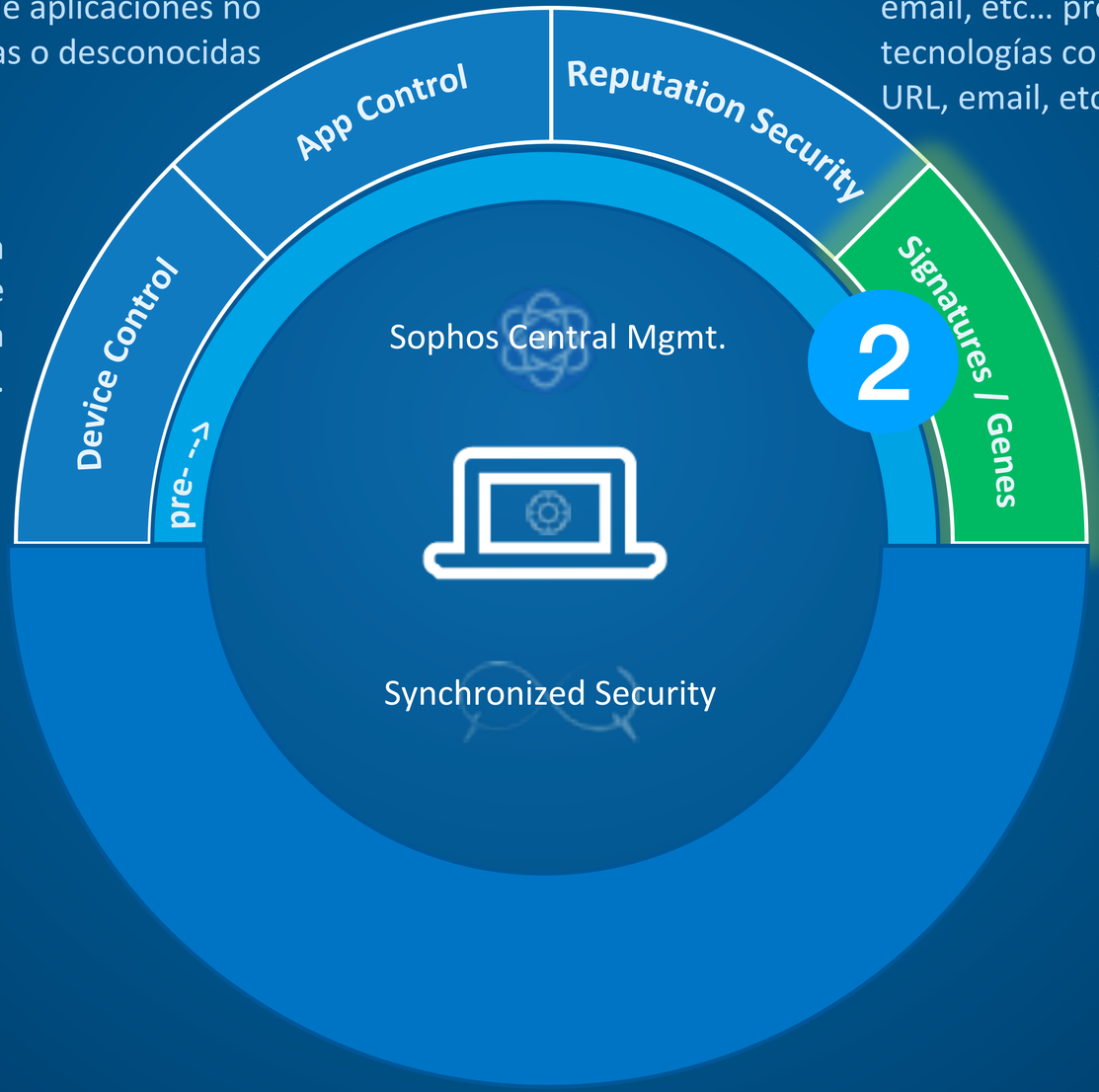
O … controlar las acciones dentro de la navegación…

sarenet

Protección Endpoint Tradicional

Para servidores o puestos, App Control previene de la ejecución de aplicaciones no deseadas o desconocidas

Control de políticas para dispositivos extraíbles para que éstos no pongan en riesgo la corporación.



Conociendo el origen/reputación de un fichero, URL, email, etc… previene ataques antes que sucedan. Incluye tecnologías como MTD, reputación de descarga, filtrado URL, email, etc…

Detección de scripts, macros, documentos y malware como primera línea eficiente de defensa contra variantes conocidas,

.exe Malware

.doc .xls .pdf

Non-.exe Malware

Script-based Malware

Phishing Attacks

Malicious URLs

Removable Media

Unauthorized Apps

SOPHOS

sarenet

Machine Learning With Feature Selection Using Principal Component Analysis for Malware Detection: A Case Study

SophosLabs Matrix Report

SophosLabs 2019 Threat Report

MLPdf: An Effective Machine Learning-Based Approach for PDF Malware Detection

Today's Malware

Real-time data on the top malware threats from our award-winning SophosLabs Team. More

DocDl ▼ JSDldr ▼ Agent ▼ DrodZp ▼
Equatio ▲ Zbot ▼ Phish ▼ Upatre ▼

Today's Spam Threats

We monitor spam from all sources, every day. View our spam dashboard for real-time data. More

PdfUri ▼ 20180802 FareitVB ▲ RtfExp ▼
▲ DrodGzip ▲ Iframe ▲
BredoZp ▲ DrodZp ▼

Tweets by @SophosLabs

SophosLabs
@SophosLabs

More about #OldPhantomCrypter... The license for this kit can be purchased via the main distribution web page for $199 per month, which positions it in the league of the most expensive builders in the market.

See more in our technical paper: news.sophos.com/en-us/2019/02/...

Adware and PUAs

Controlled Applications

sarenet

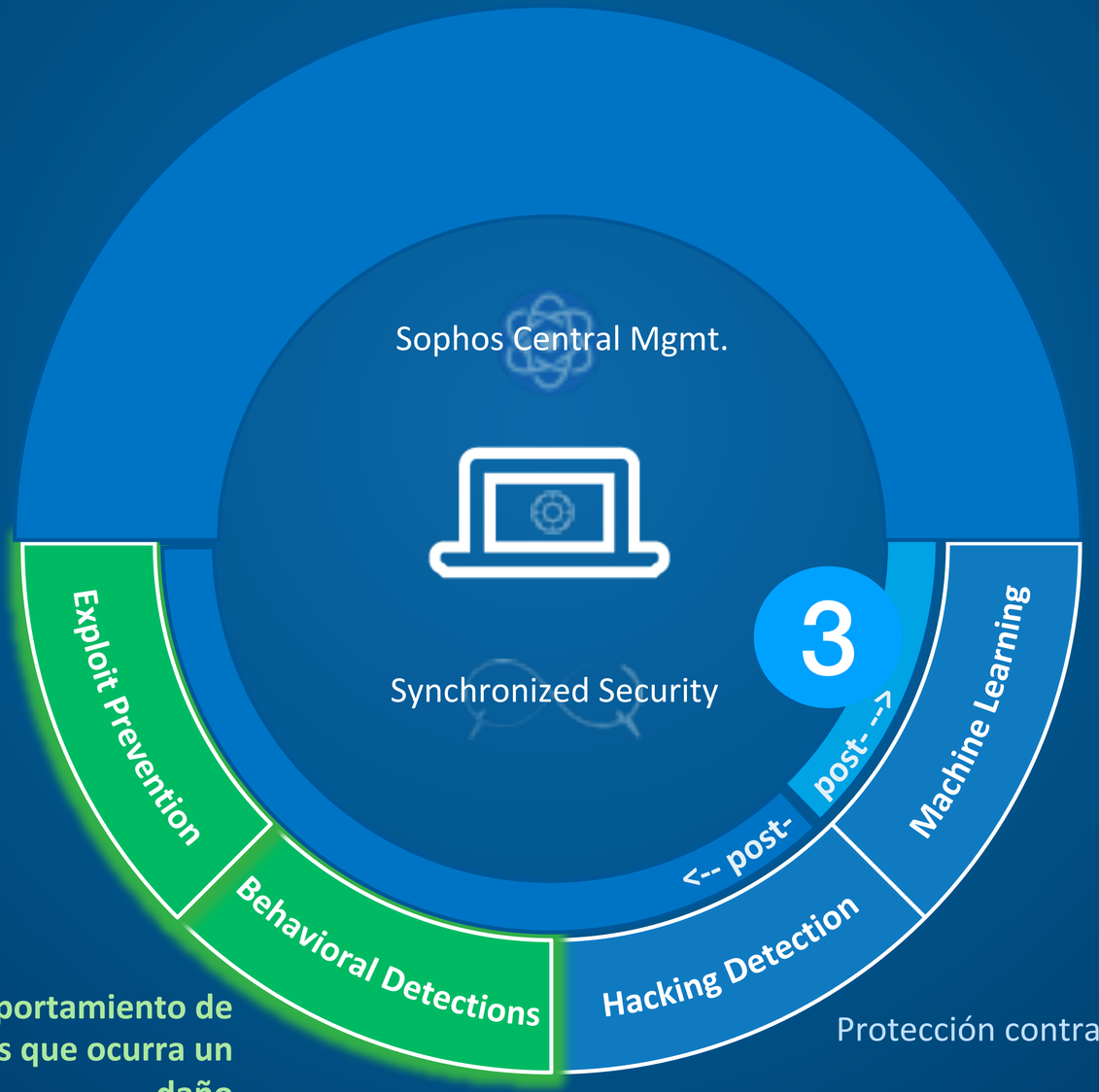
Protección EndPoint de Nueva Generación

Ramsomware

.doc
.xls
.pdf
CodeCaves

Hacking

Detección en tiempo de ejecución contra exploits y ransomware basándose en comportamiento. Proporciona características NextGen con capacidad de análisis forense de Causa Raíz (RCA).



Privilegios

Exploits

Credenciales

Tools

A través de Invincea, en pre-ejecución, detección de amenazas no conocidas gracias a su tecnología líder de ML con baja tasa de falso positivo, haciéndola única.

Detección heurística basada en el comportamiento de ejecución para eludir técnicas evasivas antes que ocurra un daño

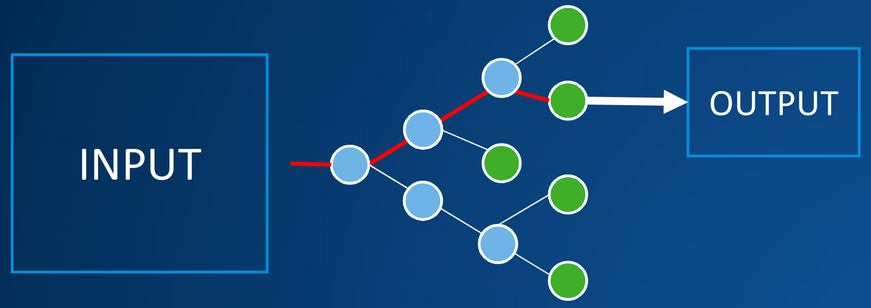
Protección contra técnicas post-explotación

SOPHOS

sarenet

Machine Learning Vs. Deep Learning

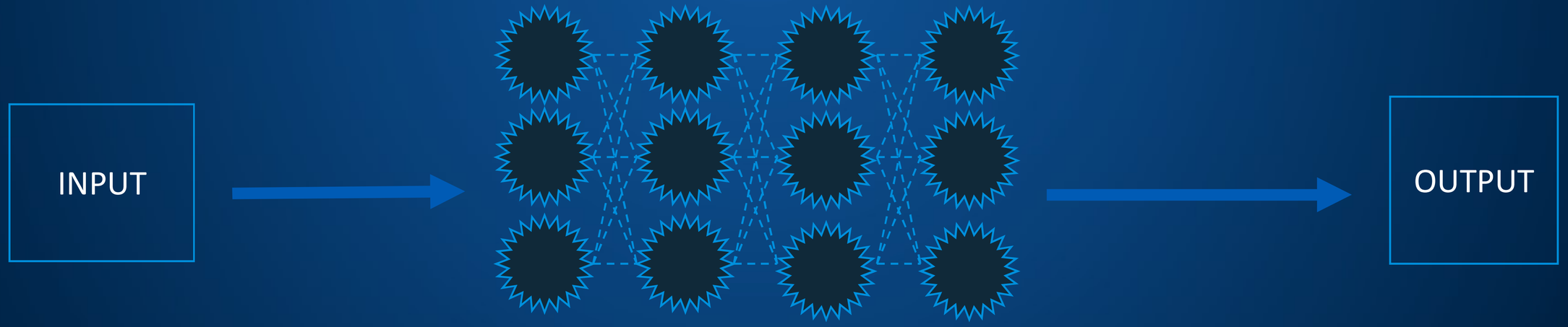
MACHINE LEARNING



Decision Tree

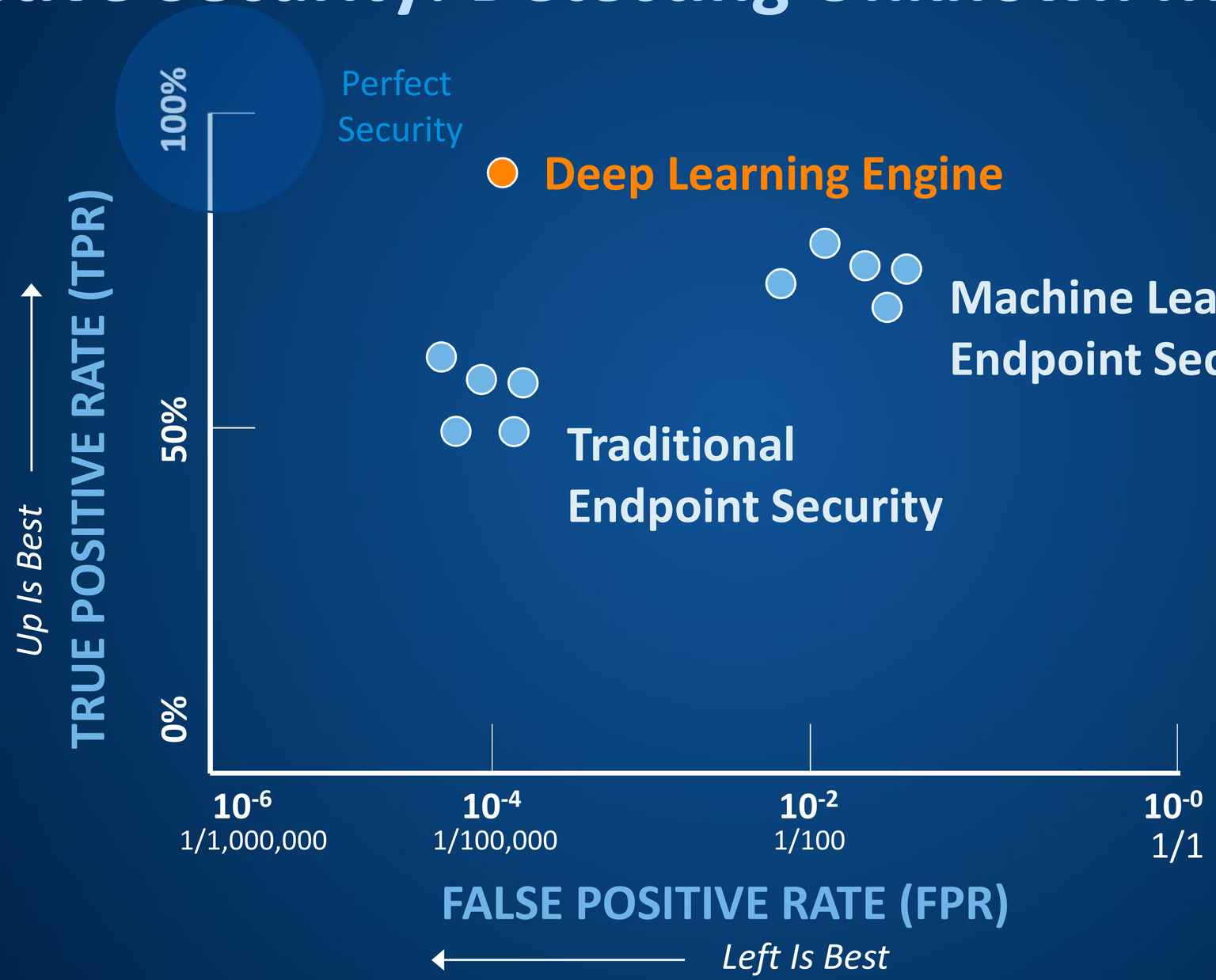
Random Forest

DEEP LEARNING



Interconnected Layers of Neurons, Each Identifying More Complex Features

Predictive Security: Detecting Unknown Malware



Source: SophosLabs analysis of malware found in the wild

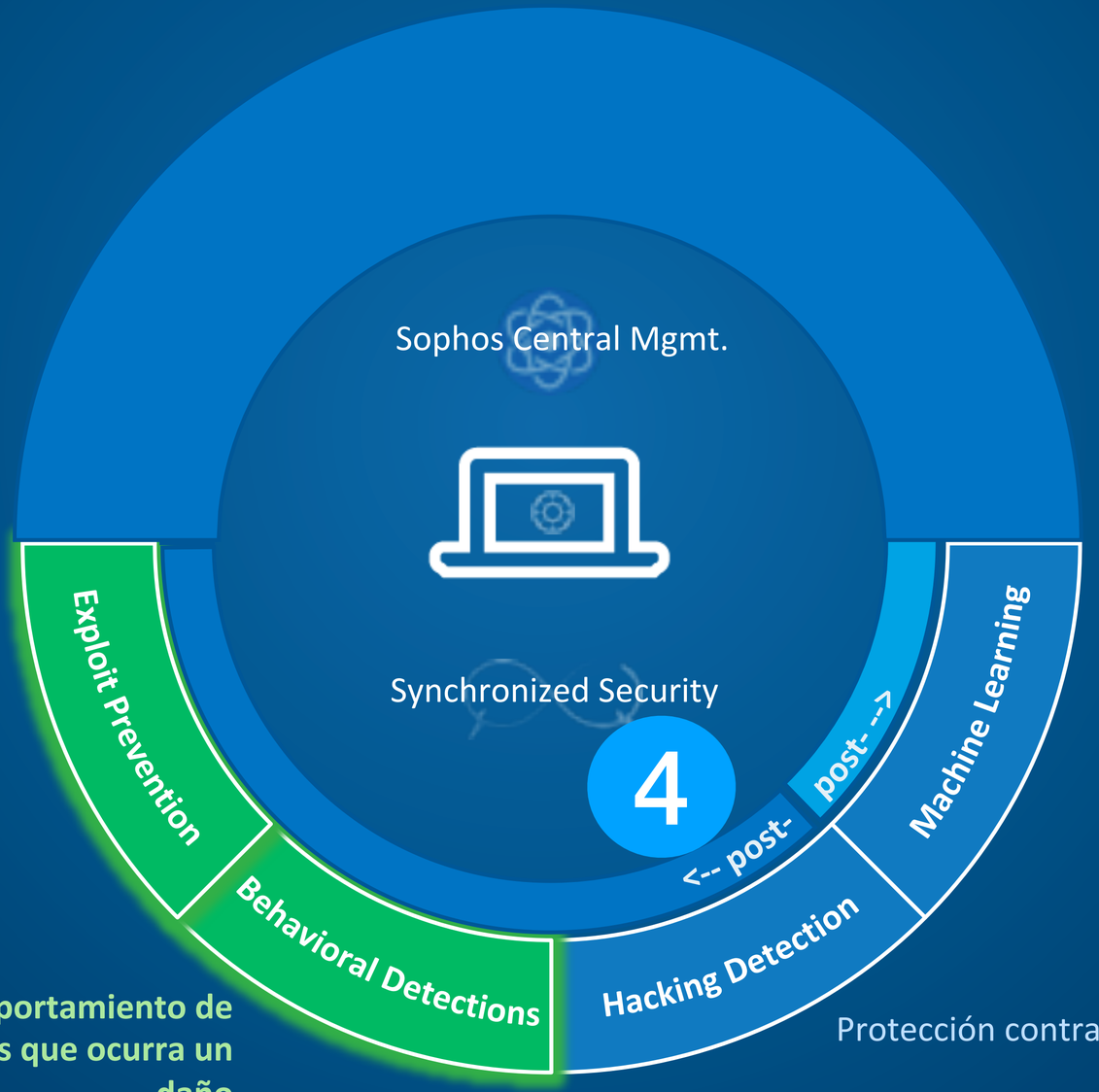
Protección EndPoint de Nueva Generación

Ramsomware

.doc
.xls
.pdf
CodeCaves

Hacking

Detección en tiempo de ejecución contra exploits y ransomware basándose en comportamiento. Proporciona características NextGen con capacidad de análisis forense de Causa Raíz (RCA).



Privilegios

Exploits

Credenciales

Tools

A través de Invincea, en pre-ejecución, detección de amenazas no conocidas gracias a su tecnología líder de ML con baja tasa de falso positivo, haciéndola única.

Detección heurística basada en el comportamiento de ejecución para eludir técnicas evasivas antes que ocurra un daño

Protección contra técnicas post-explotación

SOPHOS

sarenet

Protección incluso cuando ya se ha vulnerado

4

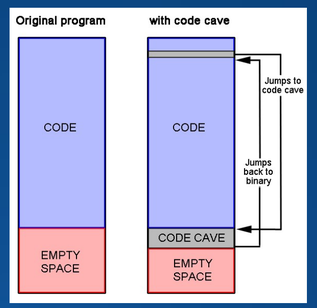
Credential Theft Protection

- Prevent dumping of credentials from memory
- Protect the credential database on Disk and Registry

Additional Registry Protections

- Sticky Key Mitigation
- Application Verifier Protection (Double Agent)

Active Adversary protections



- Code Cave prevention
- Malicious Process Migration
- Process privilege escalation
- APC Filter (prevent Atom Bombing exploit variants)
- Improved Application Lockdown
  - Powershell abuse from browsers
  - HTA apps

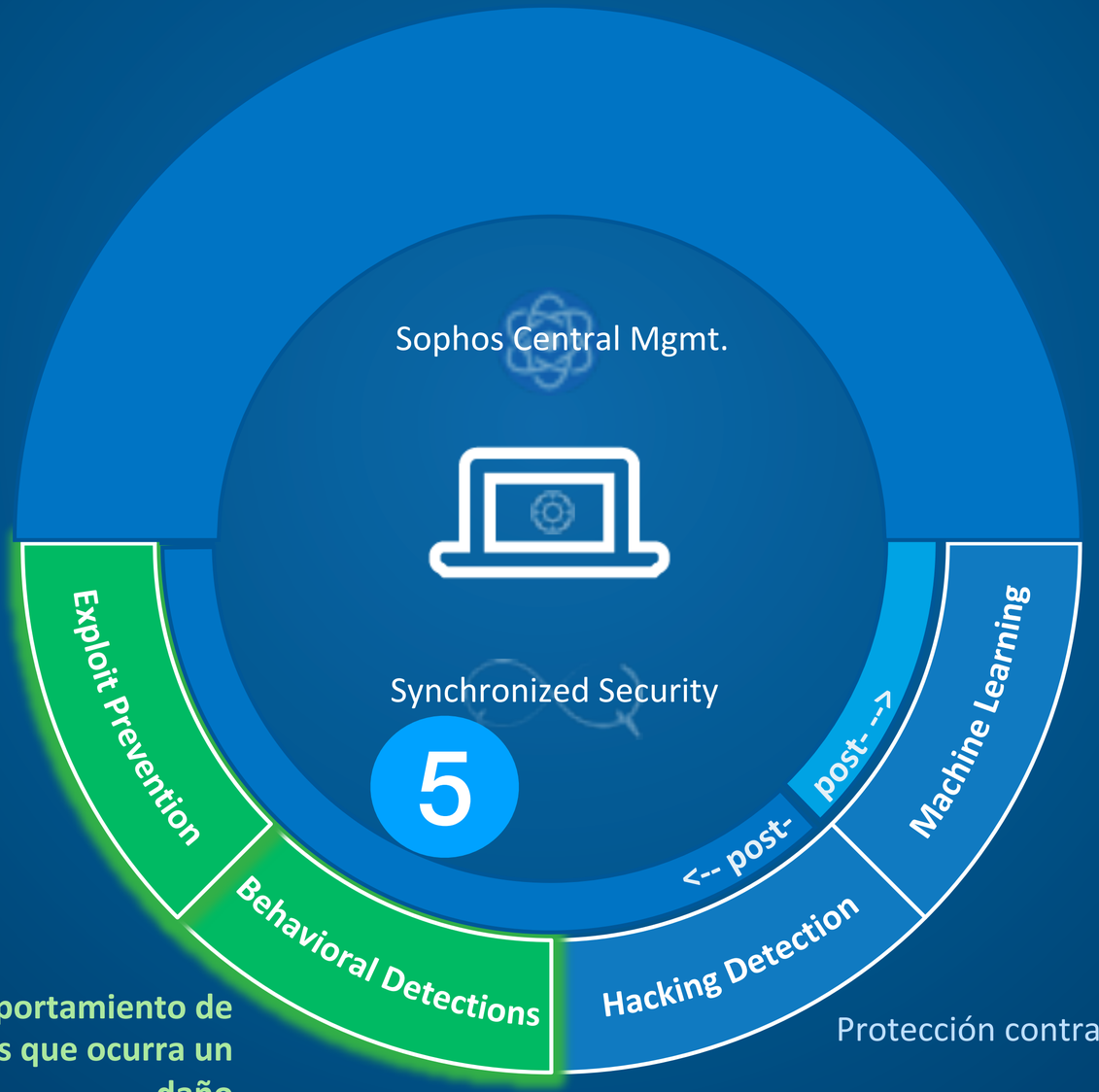
Protección EndPoint de Nueva Generación

Ramsomware

.doc
.xls
.pdf
CodeCaves

Hacking

Detección en tiempo de ejecución contra exploits y ransomware basándose en comportamiento. Proporciona características NextGen con capacidad de análisis forense de Causa Raíz (RCA).



Privilegios

Exploits

Credenciales

Tools

A través de Invincea, en pre-ejecución, detección de amenazas no conocidas gracias a su tecnología líder de ML con baja tasa de falso positivo, haciéndola única.

Detección heurística basada en el comportamiento de ejecución para eludir técnicas evasivas antes que ocurra un daño

Protección contra técnicas post-explotación

SOPHOS

sarenet

InterceptX vs Ransomware = CryptoGuard + WipeGuard

File Protection

Stops Techniques That Encrypt or Compress Files

Disk and Boot Record Protection

Stops Advanced Attacks that attempt to Lock a device pre-OS

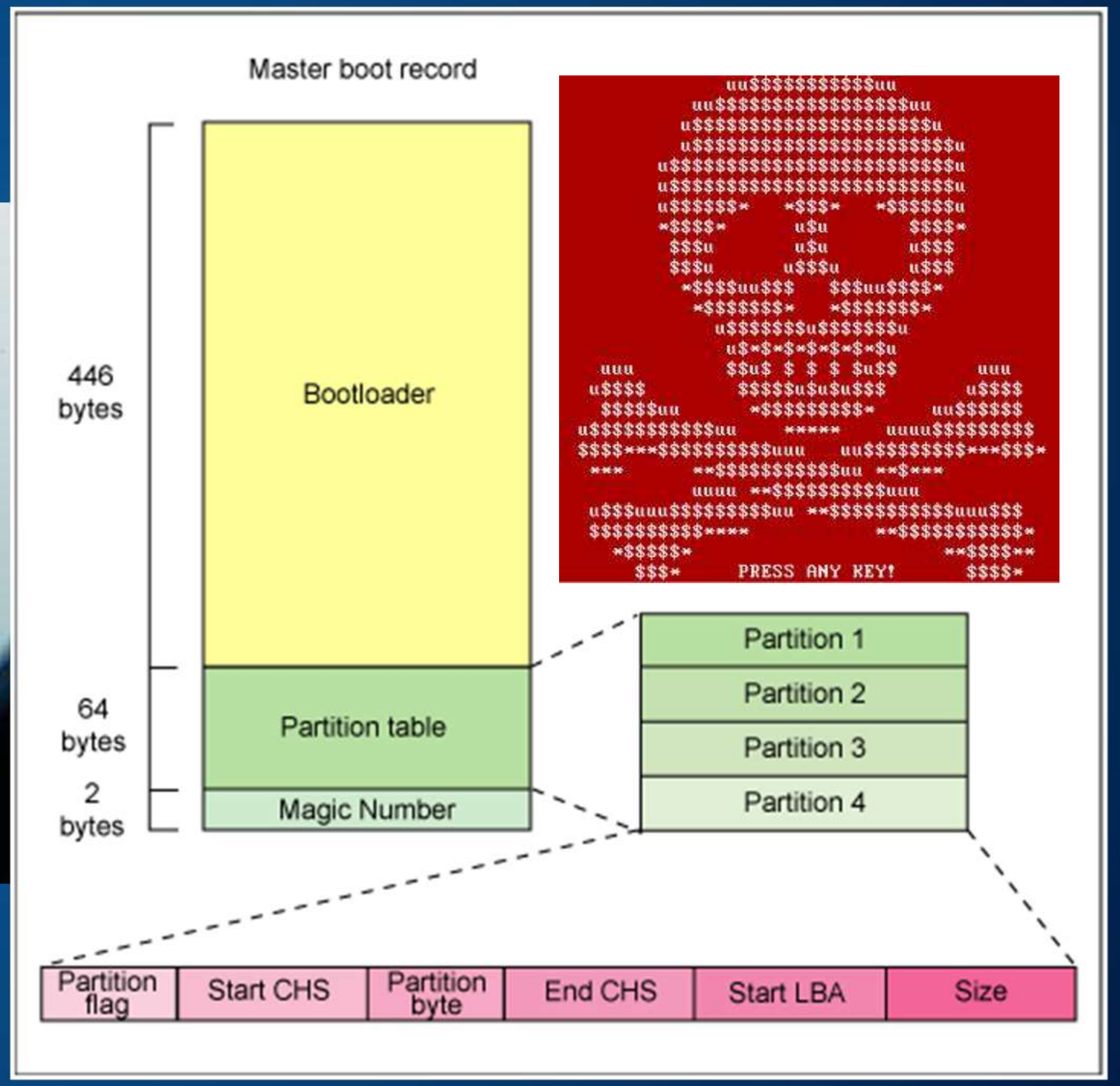
Memory Protection

Stops Memory Exploits From Starting an Encryption Process

CryptoGuard – Interceptando Ransomware

WipeGuard: Modificación MBR

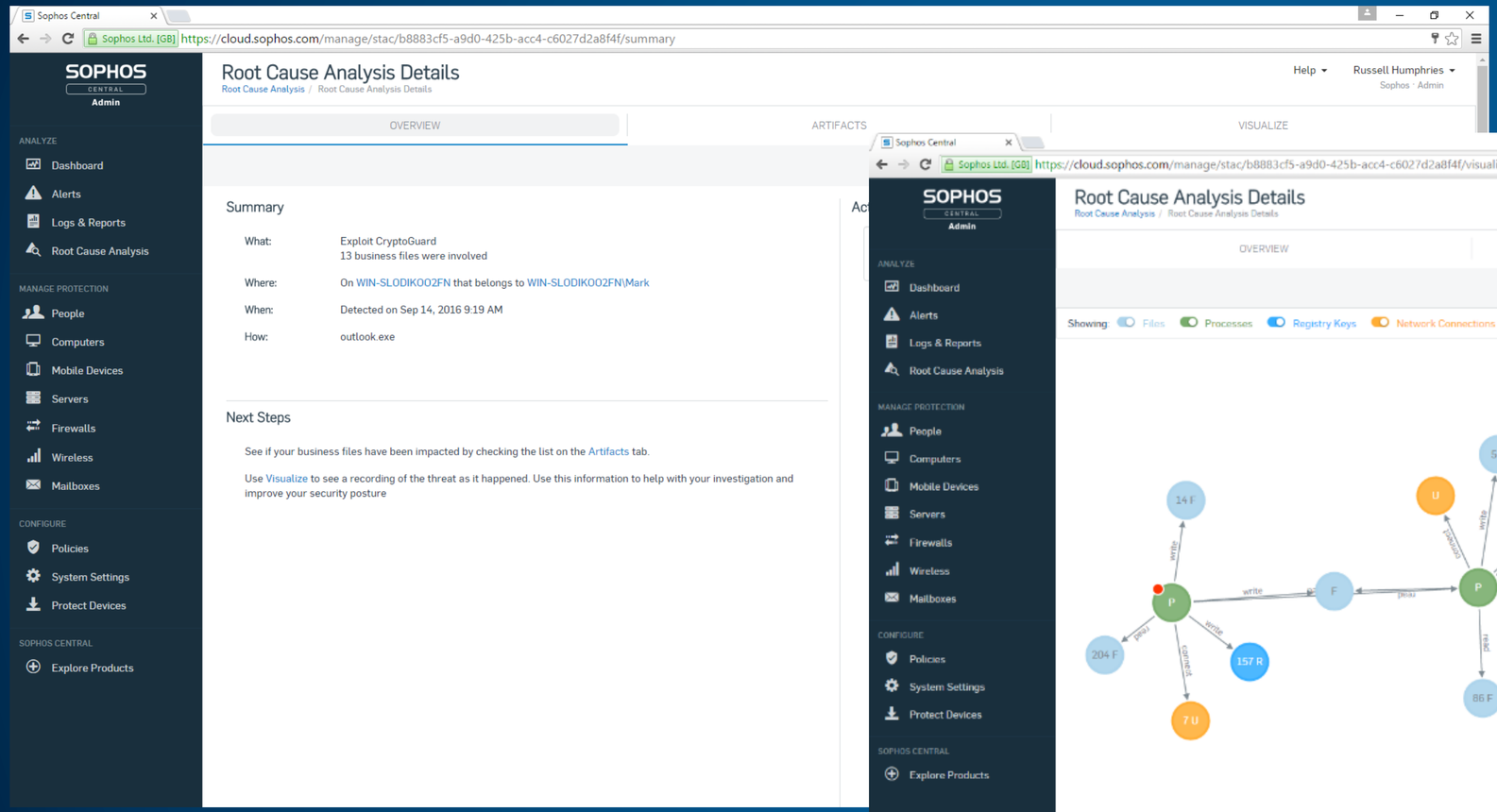
Master Boor Record
Registro de arranque maestro

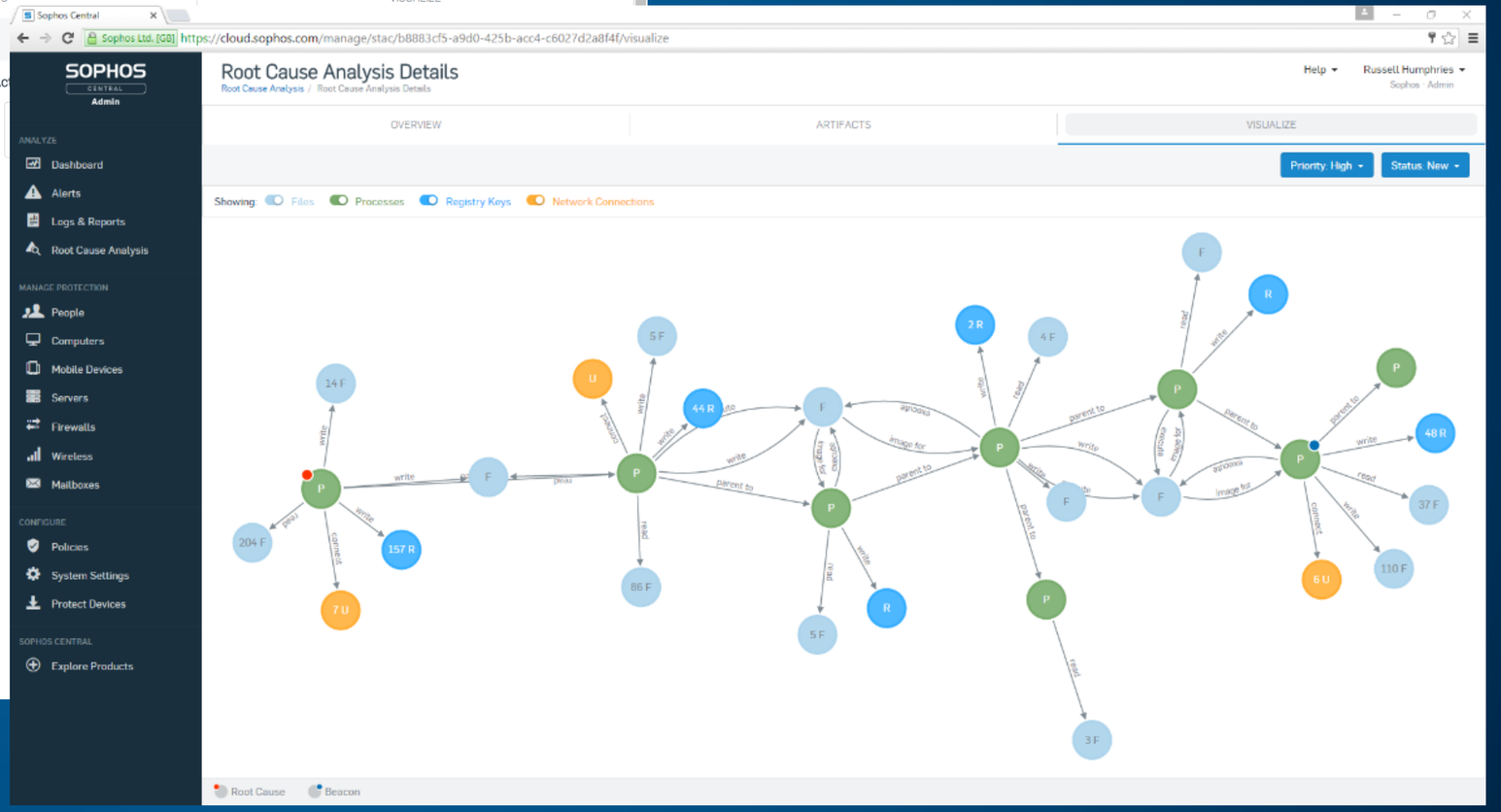


Analisis de causa raiz

Entendiendo el Quién, Qué, Cuándo, Dónde, Por qué y Cómo

5





SOPHOS

sarenet

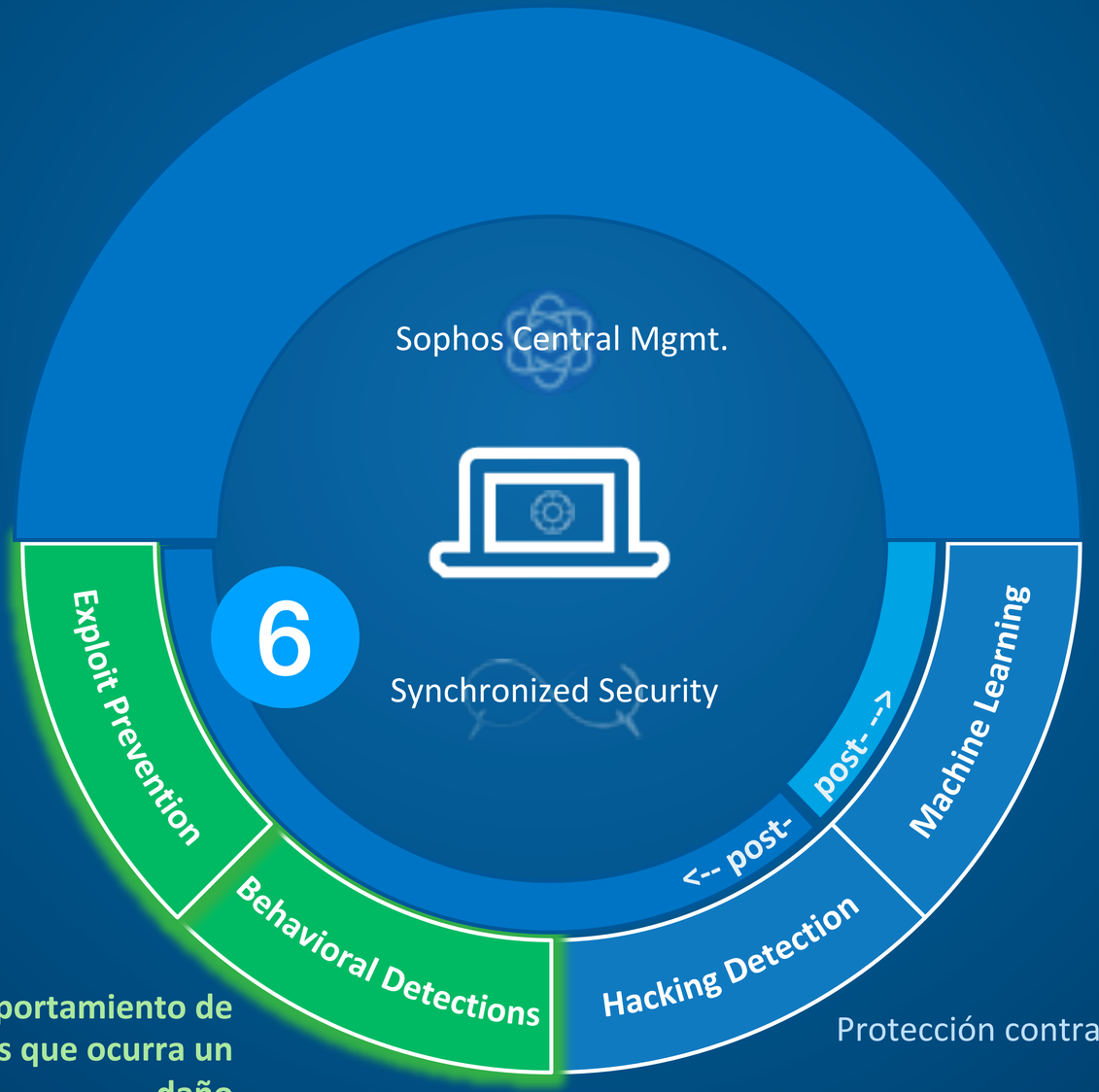
Protección EndPoint de Nueva Generación

Ramsomware

.doc
.xls
.pdf
CodeCaves

Hacking

Detección en tiempo de ejecución contra exploits y ransomware basándose en comportamiento. Proporciona características NextGen con capacidad de análisis forense de Causa Raíz (RCA).



Privilegios

Exploits

Credenciales

Tools

A través de Invincea, en pre-ejecución, detección de amenazas no conocidas gracias a su tecnología líder de ML con baja tasa de falso positivo, haciéndola única.

Detección heurística basada en el comportamiento de ejecución para eludir técnicas evasivas antes que ocurra un daño

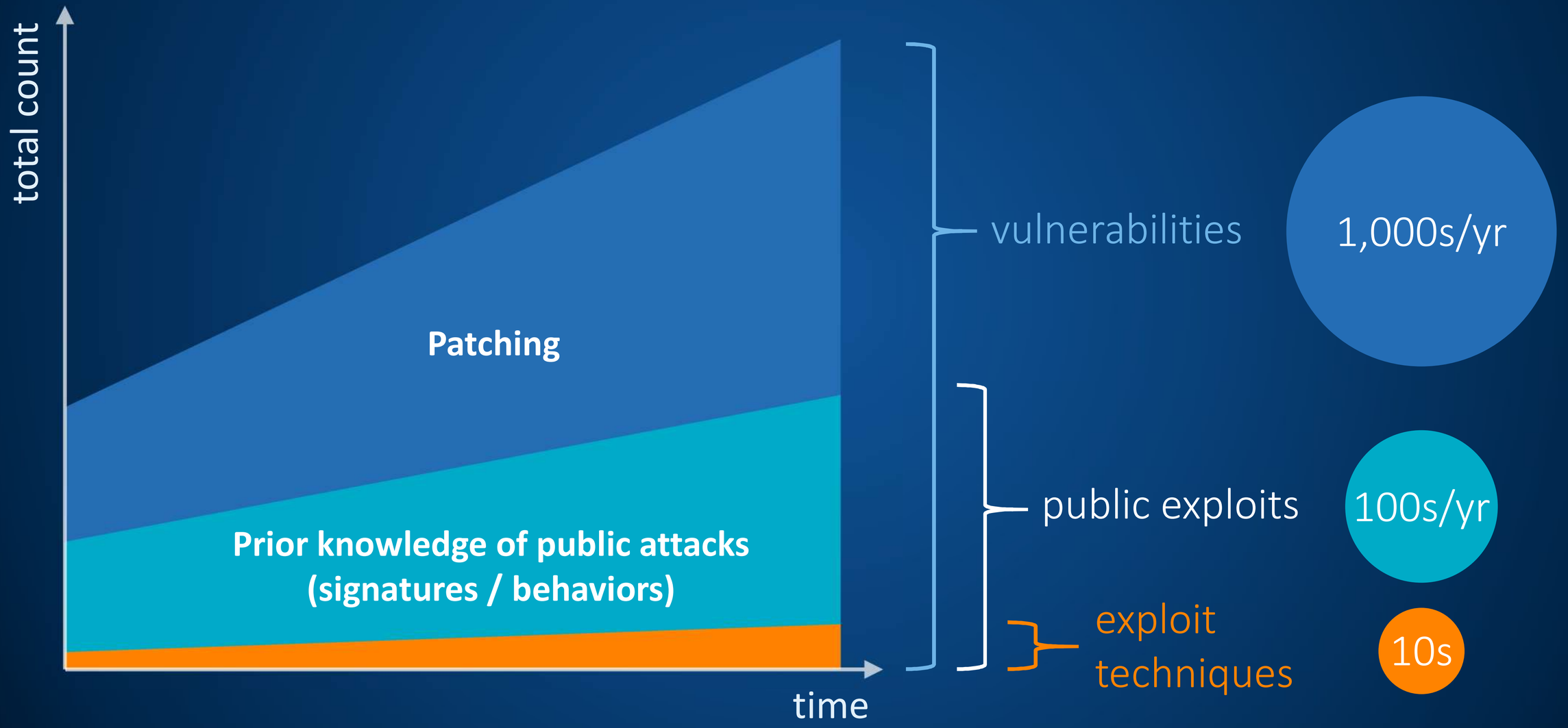
Protección contra técnicas post-explotación

SOPHOS

sarenet

Cómo podemos interceptar un Exploit

Vulnerabilities vs Exploits vs Exploit Techniques



Some of the Exploit and Active Adversary Techniques Stopped by Intercept X

Enforce data execution prevention	Mandatory address space layout randomization	Bottom-up ASLR	Null page deference	Heap spray allocation	Dynamic heap spray	Stack pivot and stack exec (memory protection)
Stack-based ROP (caller)	Structured exception handling overwrite (SEHOP)	Import address table faltering (IAF)	Load library	Reflective DLL injection	Malicious shellcode	VBScript god mode
WOW64	Syscall	Hollow process	DLL hijacking	Squiblydoo Applocker bypass	APC protection (Double Pulsar / Atom Bombing)	Process privilege escalation
	Credential theft protection	Code cave mitigation	MITB protection (Safe Browsing)	Malicious traffic detection	Meterpreter shell detection	

Protección EndPoint de Nueva Generación

Para servidores o puestos, App Control previene de la ejecución de aplicaciones no deseadas o desconocidas

Conociendo el origen/reputación de un fichero, URL, email, etc… previene ataques antes que sucedan. Incluye tecnologías como MTD, reputación de descarga, filtrado URL, email, etc…

.exe Malware

Non-.exe Malware

Script-based Malware

Phishing Attacks

Control de políticas para dispositivos extraíbles para que éstos no pongan en riesgo la corporación.

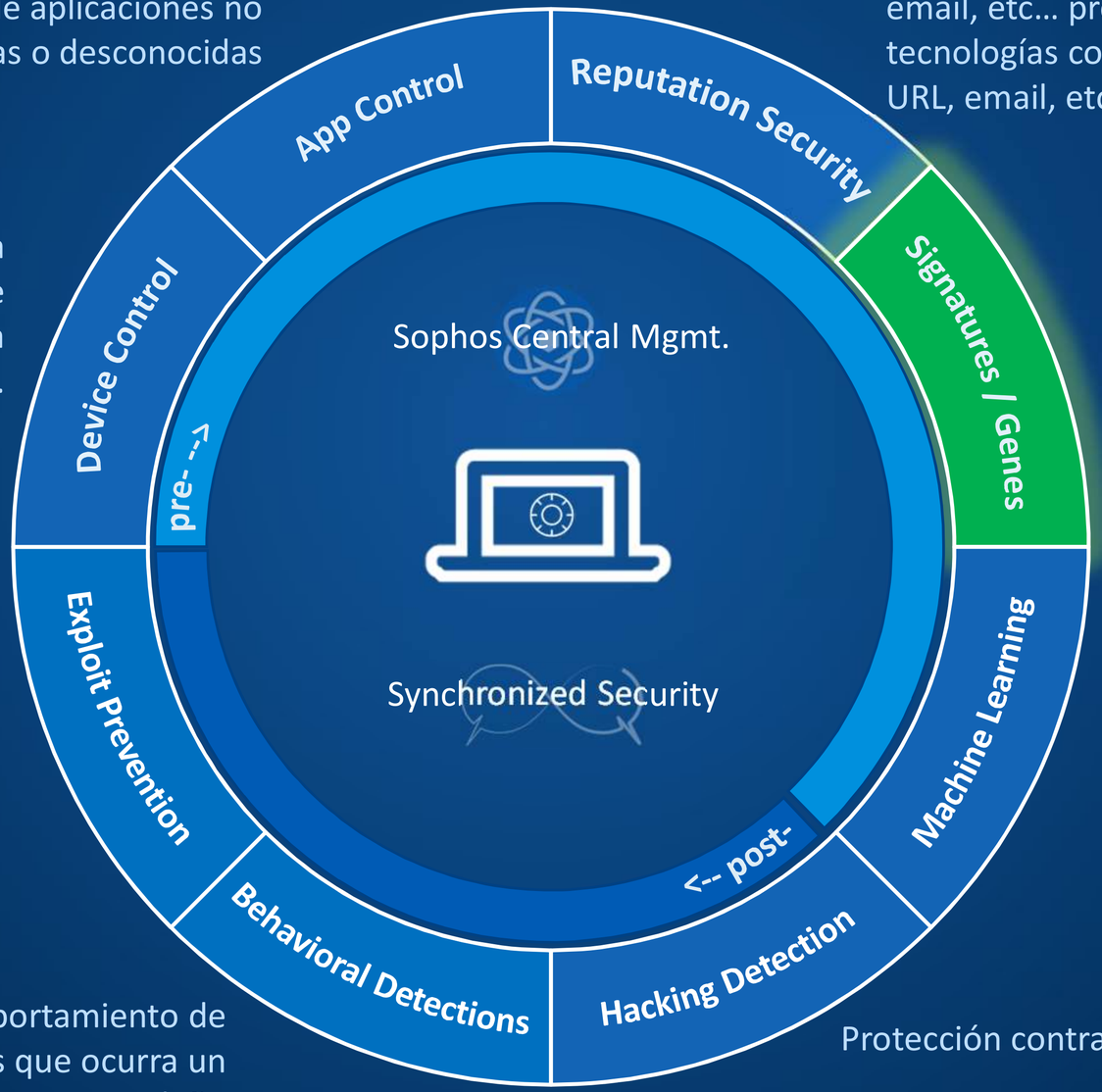
Detección de scripts, macros, documentos y malware como primera línea eficiente de defensa contra variantes conocidas,

Malicious URLs

Exploits

Removable Media

Unauthorized Apps



Detección en tiempo de ejecución contra exploits y ransomware basándose en comportamiento. Proporciona características NextGen con capacidad de análisis forense de Causa Raíz (RCA).

A través de Invincea, en pre-ejecución, detección de amenazas no conocidas gracias a su tecnología líder de ML con baja tasa de falso positivo, haciéndola única.

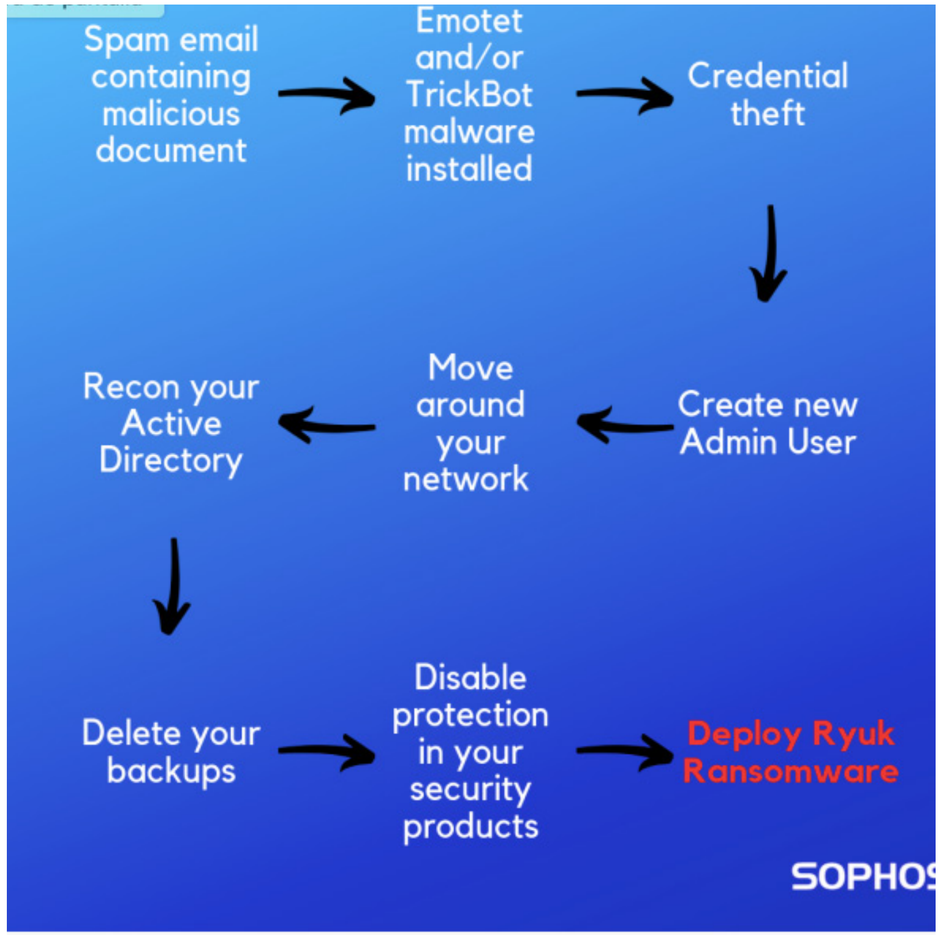
Detección heurística basada en el comportamiento de ejecución para eludir técnicas evasivas antes que ocurra un daño

Protección contra malware basado en memoria.

SOPHOS

sarenet

Parar Ryuk con Sophos Intercept X Advanced



- Detectar y bloquear las técnicas de explotación utilizadas para descargar e instalar Emotet y Trickbot (a menudo a través de PowerShell o WMI), evitando que los piratas informáticos entren en su red.
- Prevenir el robo de credenciales, deteniendo así el acceso no autorizado a sus sistemas y la escalada de privilegios de administrador.
- Detener la ejecución del ransomware examinando su “ADN” con nuestra red neuronal de aprendizaje profundo.
- Detectar y deshacer el cifrado no autorizado de archivos a través de las capacidades de CryptoGuard

PROTECCIÓN AVANZADA CON APRENDIZAJE MEDIANTE DEEP LEARNING DE TÉCNICAS Y COMPORTAMIENTOS DE ATAQUE				PROTECCIÓN TRADICIONAL CON FICHEROS POR FIRMAS
	Sophos Intercept X Advanced with EDR	**Sophos Intercept X Advanced**	**Sophos Intercept X**	**Sophos Endpoint Protection**
Técnicas base	✔	✔		✔
Deep Learning	✔	✔	✔	
Antiexploits	✔	✔	✔	
Antiransomware de CryptoGuard	✔	✔	✔	
Detección y respuesta para endpoints (EDR)	✔			

SOPHOS

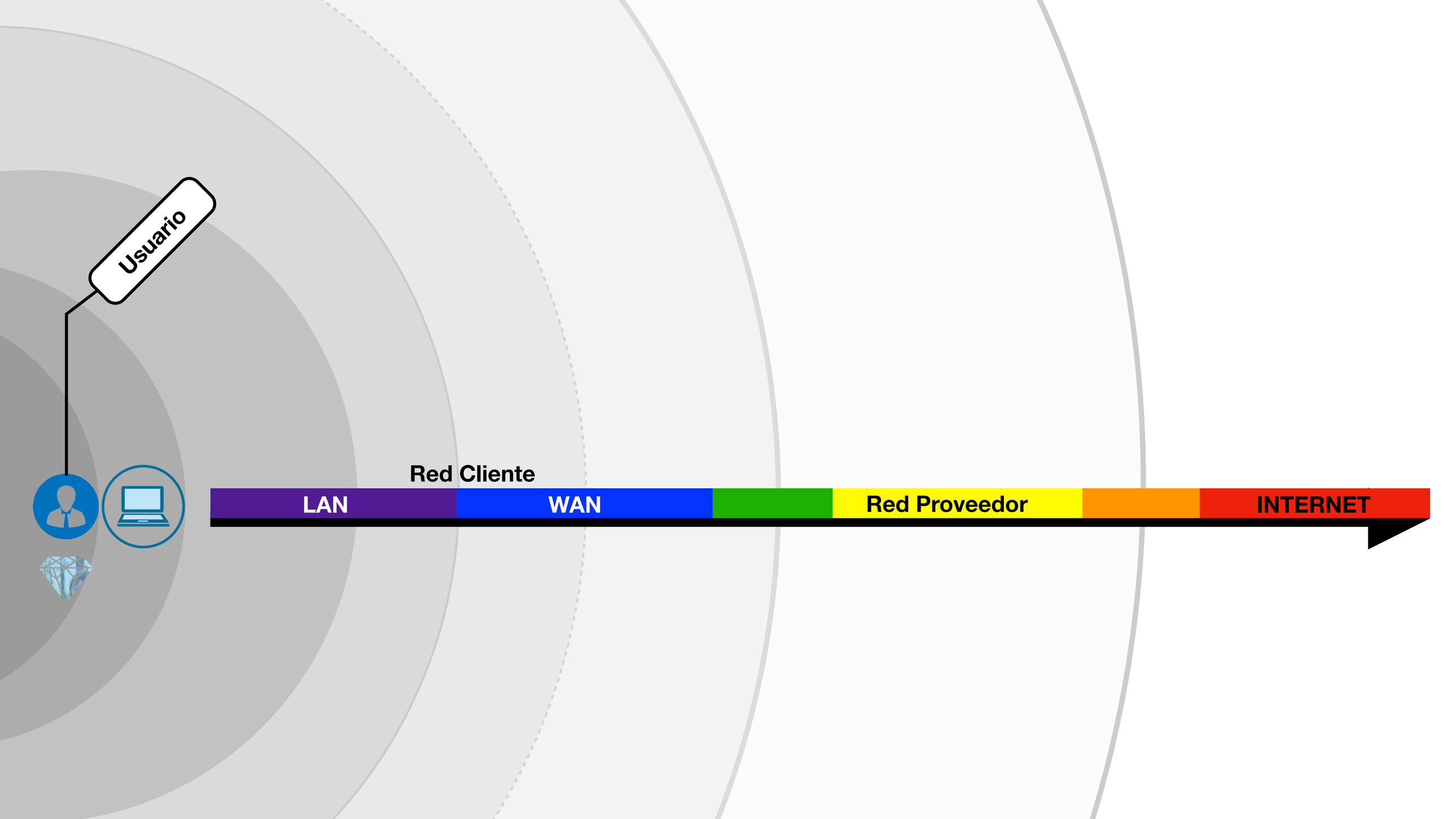
sarenet

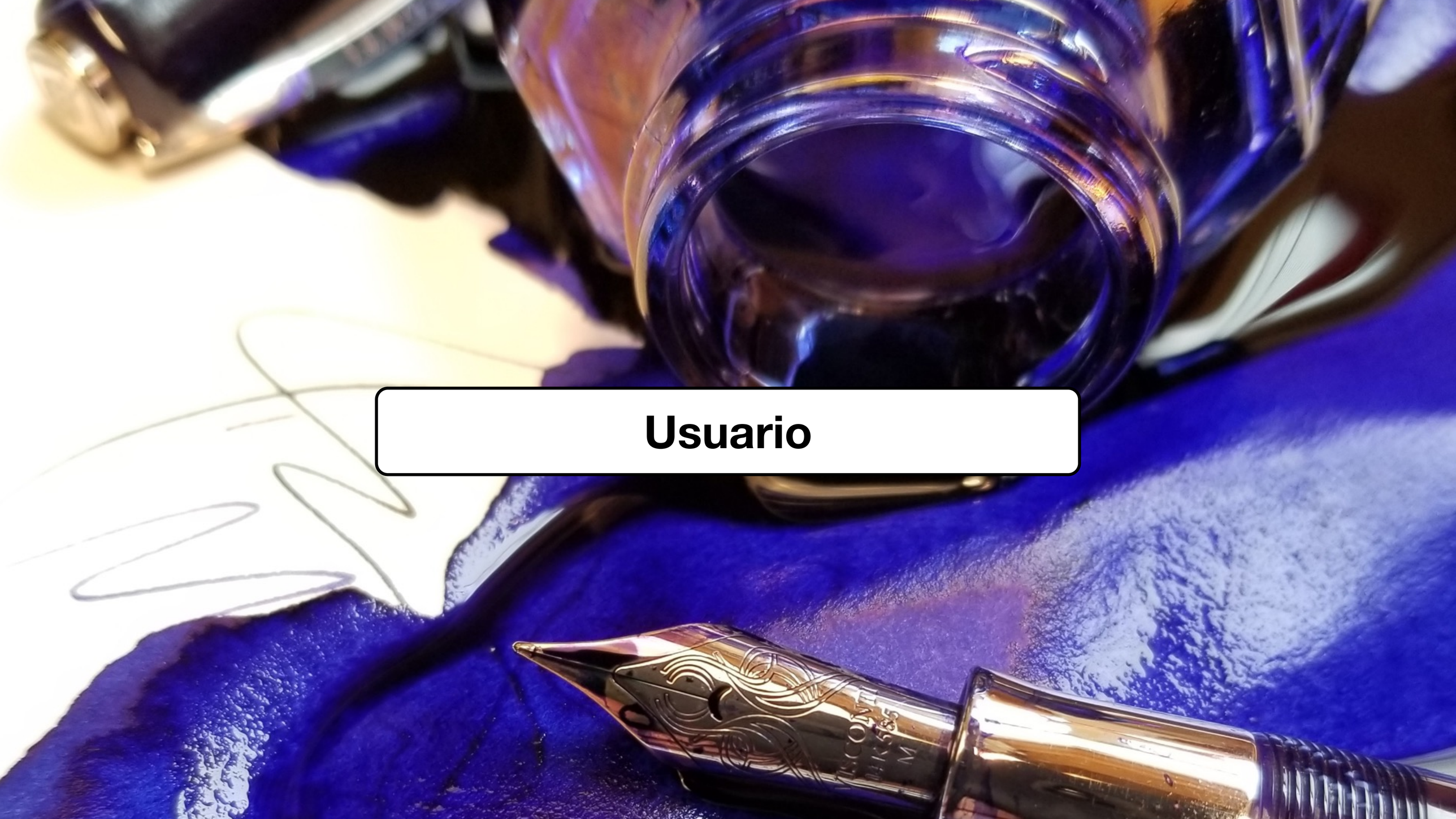
RESUMEN DE LAS CARACTERÍSTICAS PRINCIPALES DE LOS ENDPOINT DE SOPHOS

- **Gestión centralizada** desde consola en la nube. 3 niveles de administración (Sarenet, Dpto. IT y usuario)
- Es un **cliente ligero** en cuanto a consumo local de recursos y sus actualizaciones no son de alto volumen
- Pago por uso en base a licencias. **Un usuario es una licencia**. Una licencia es válida para todos los PCS y portátiles del mismo usuario, no así con tablet y smartphone donde hay que ir a los productos de movilidad.
- Hay protecciones **servidor** y protecciones **puestos normales**
- Los procesos de **Deep Learning** se ejecutan en **local**, en el propio equipo, y no se requiere de Internet
- Es un tecnología **compatible con otros fabricantes AV**
- **Multiplataforma**

SOPHOS

sarenet


Usuario
Red Cliente
LAN
WAN
Red Proveedor
INTERNET


Usuario

Decanato UPV

[IMPORTANTE] Se busca propietario de vehículo

Para: info@dasphotonics.com,opeset@dasphotonics.com,apalau@dasphotonics.com

Responder a: Decanato UPV

ATENCIÓN:

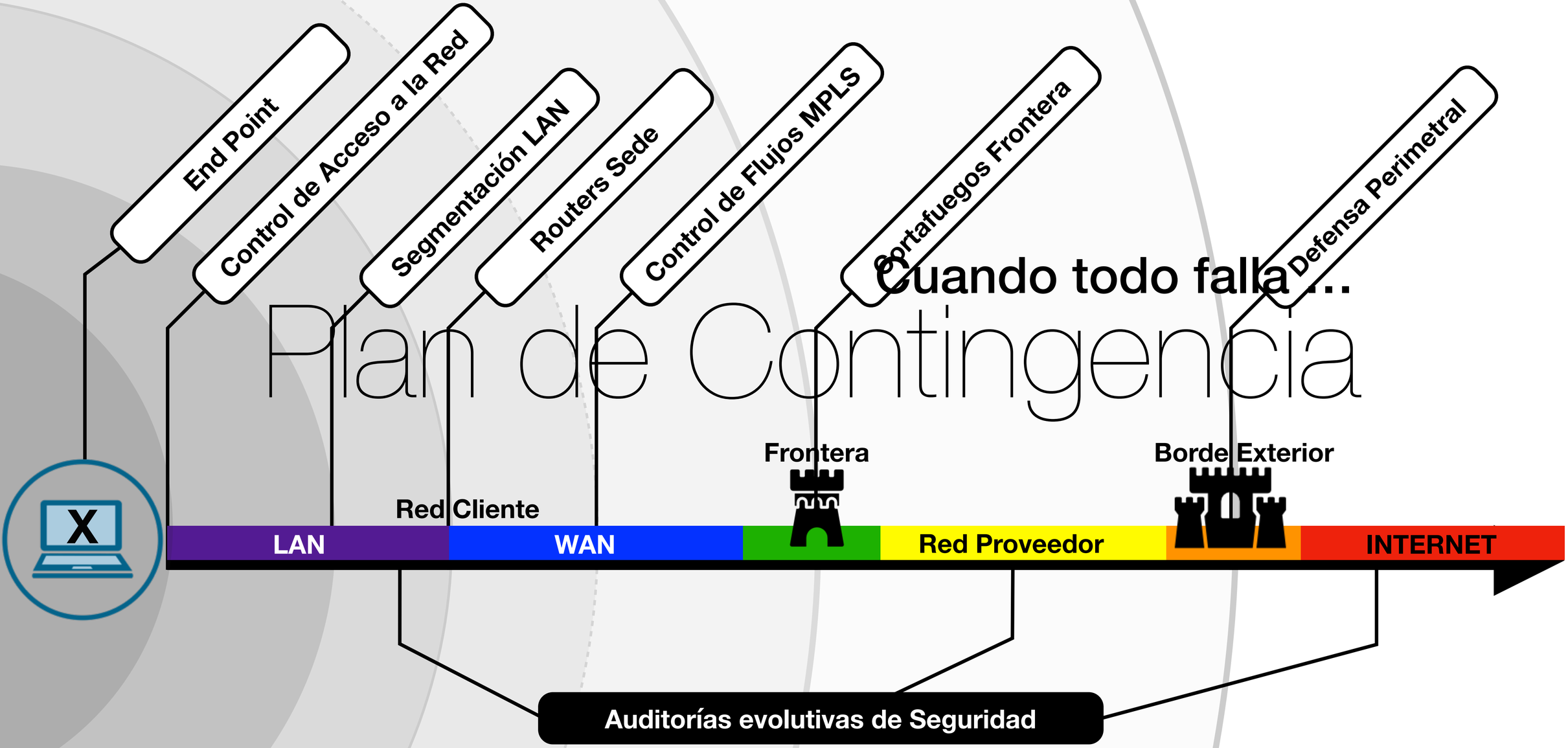
Se ha producido un pequeño accidente en el aparcamiento junto al edificio de microscopía en Camino de Vera. Estamos intentando localizar al propietario del vehículo que se ha visto afectado.

Un operario de mantenimiento nos ha facilitado una foto del coche que hemos adjuntado a este correo electrónico. Si el coche es tuyo, comunícanoslo de inmediato para realizar los trámites del parte del seguro.

Decanato UPV

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

DCO100003.jpg.docx


End Point
Control de Acceso a la Red
Segmentación LAN
Routers Sede
Control de Flujos MPLS
Cortafuegos Frontera
Defensa Perimetral
Cuando todo falla...
Plan de Contingencia
Frontera
Borde Exterior
Red Cliente
LAN
WAN
Red Proveedor
INTERNET
Auditorías evolutivas de Seguridad

Plan de Contingencia

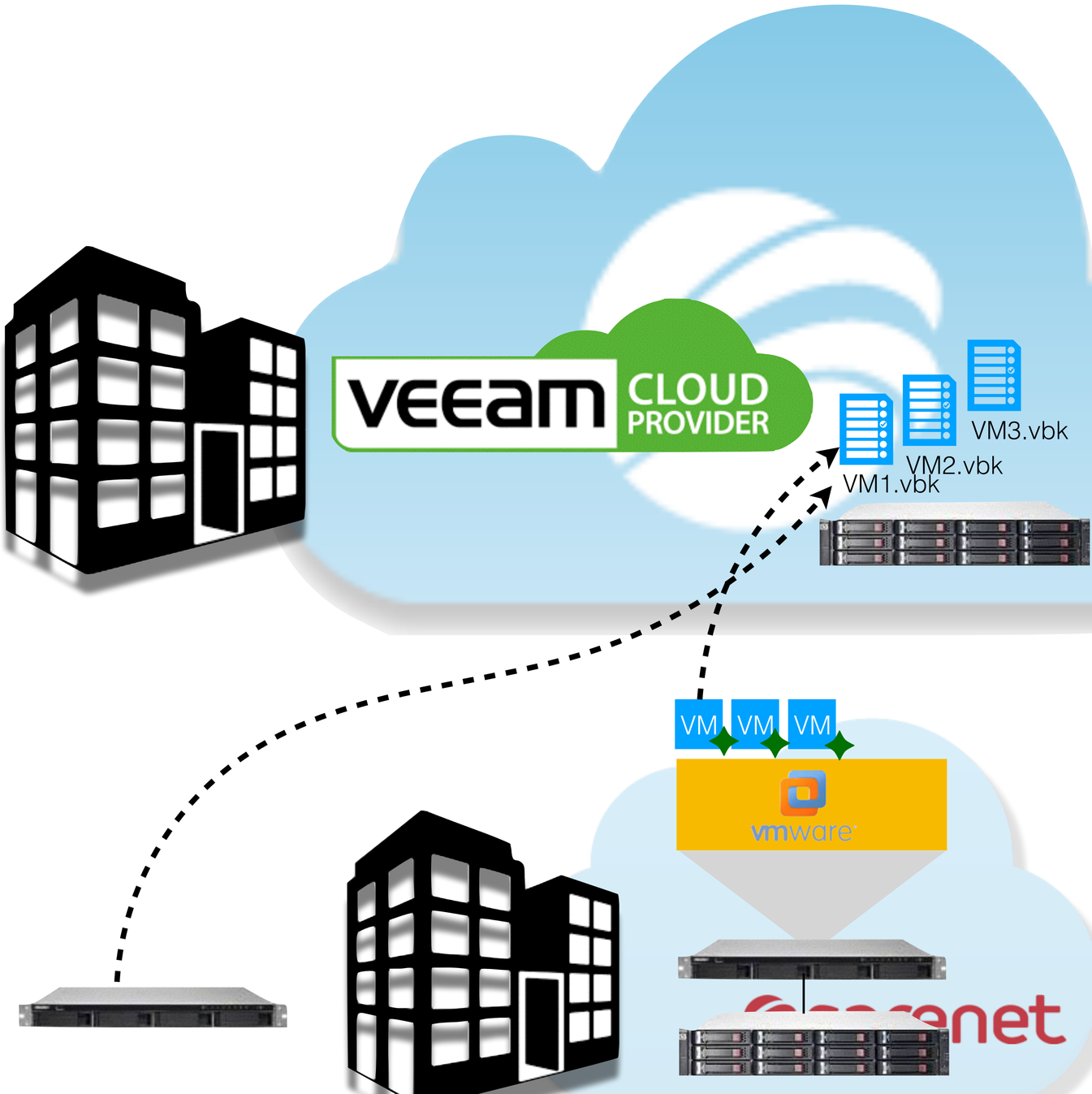
Plan de Contingencia

Veeam Cloud Connect

Veeam Cloud Connect **Backup**

Ahora, además de tener las copias generadas con Veeam en local , puedes almacenarlas fuera de tus instalaciones de forma totalmente segura

Gestiona tu conexión con este almacenamiento desde el propio Veeam y accede a tus copias y restáuralas en local cuando quieras



Plan de Contingencia

Veeam Cloud Connect

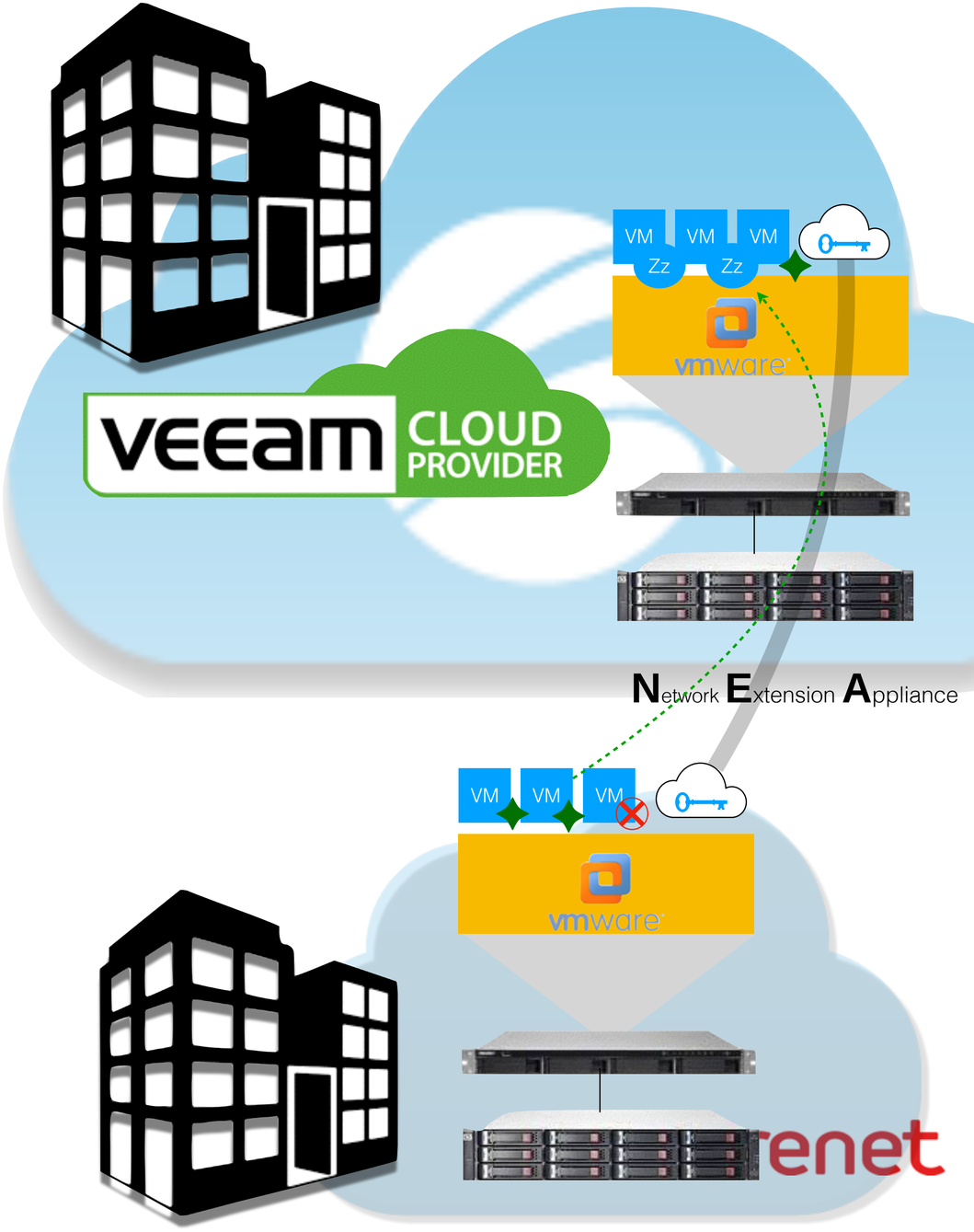
Veeam Cloud Connect **Replication**

Replica tus máquinas virtuales en un entorno externo de forma segura.

Actívalas siempre que lo necesites de forma transparente como si estuvieran en tus instalaciones con el mismo direccionamiento gracias al la tecnología NEA

Gestiona todo este proceso desde el propio Veeam

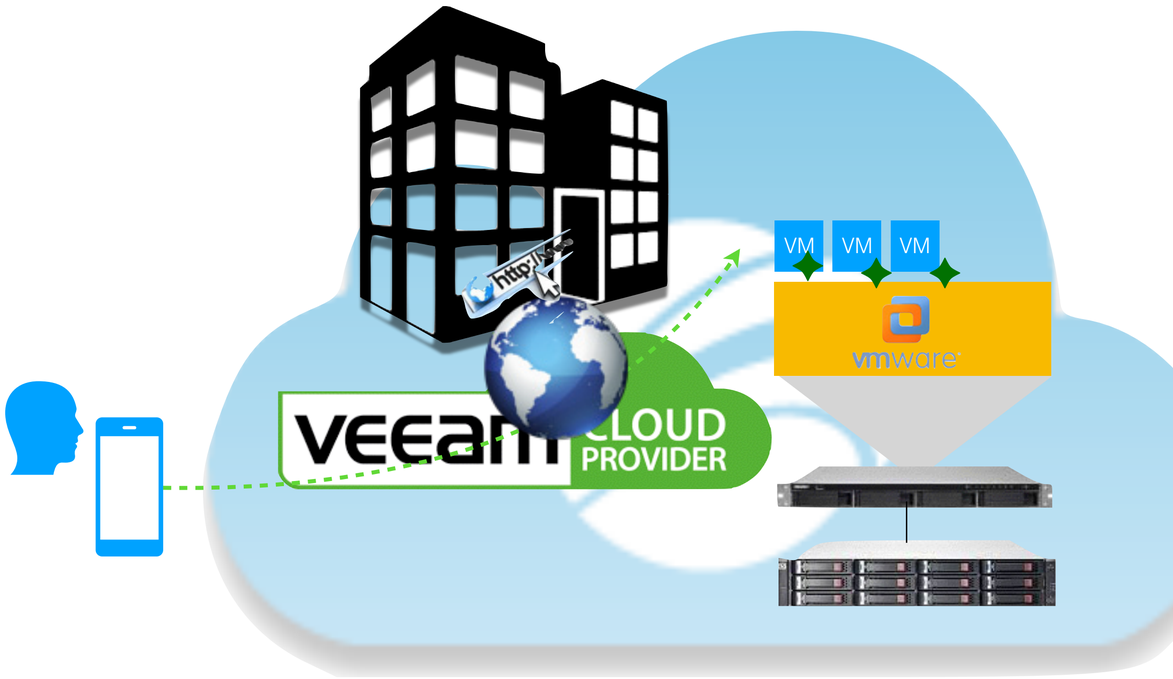
Nota: Versión vmware 5.5 o sup. , Veeam 9 ó sup.



Plan de Contingencia

Veeam Cloud Connect

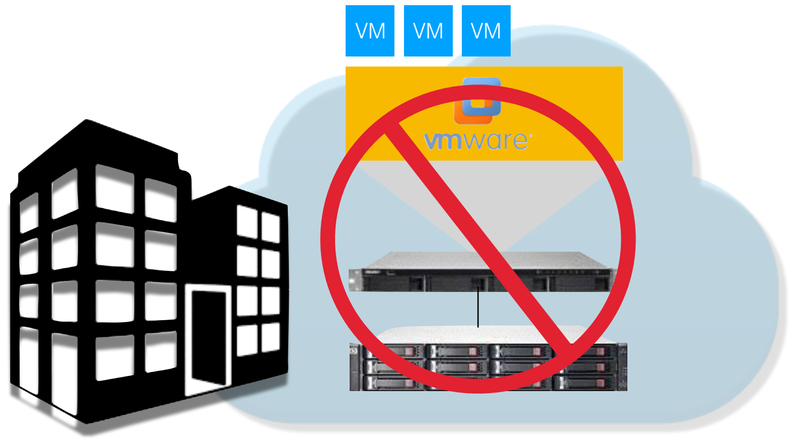
Veeam Cloud Connect Failover Plan



Replica tus máquinas virtuales en un entorno externo de forma segura.

Si tu entorno de virtualización te falla puedes tener un plan alternativo para acceder a tus máquinas por Internet

Gestiona todo este proceso desde un portal que puedes activar desde un smartphone en caso de emergencia



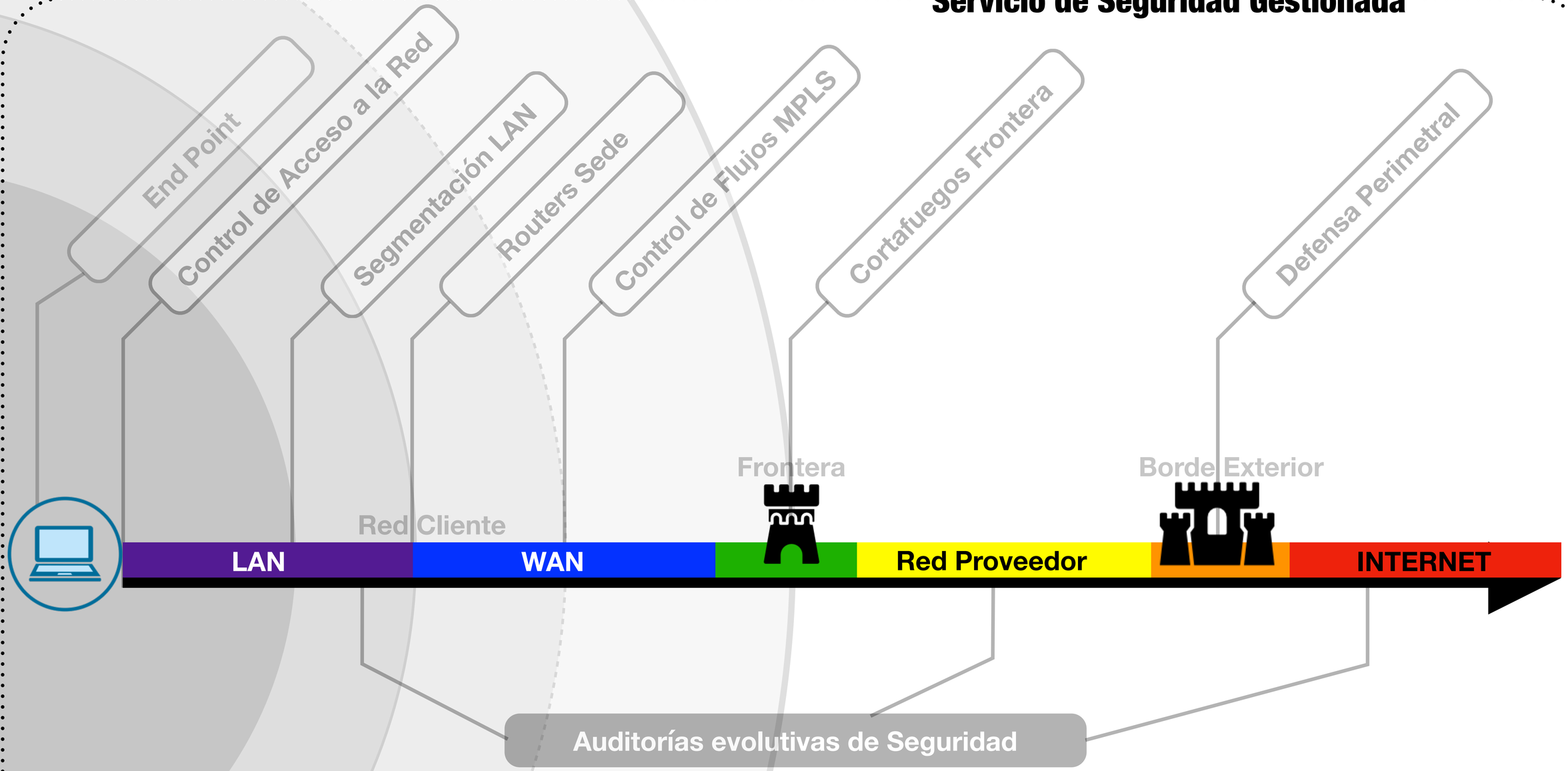
sarenet

Failover Plan

Recomendaciones generales

- Para velocidad < 100 Mbps ==> Acelerador WAN
- Versiones de Veeam y VMWare actualizadas
- Ciclos GFS con Backup Copy
- Regla 3-2-1
- Pruebas Failover Plan

Servicio de Seguridad Gestionada



Plan de Contingencia

Cuando todo falla ...

Seguridad Gestionada

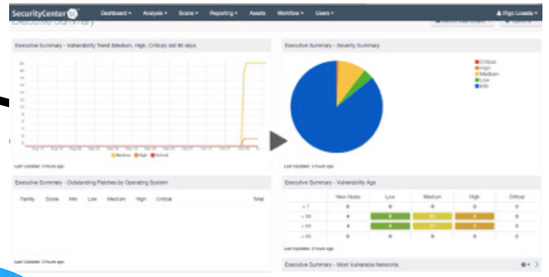
Vigilancia de alertas

Generación de informes

Monitorización de la MPLS

Cortafuegos

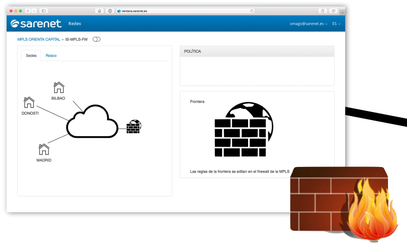
Sistema de análisis de vulnerabilidades Security Center



Frontera

Gestión de redes Wifi

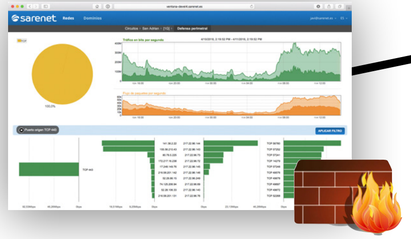
Control de flujos



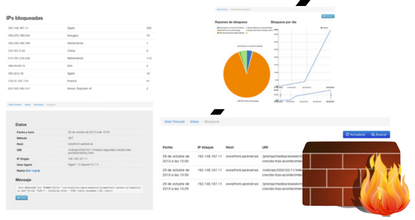
Actuaciones sobre activos

Segmentación y segregación de la red

Perimetral DDoS



Aplicaciones



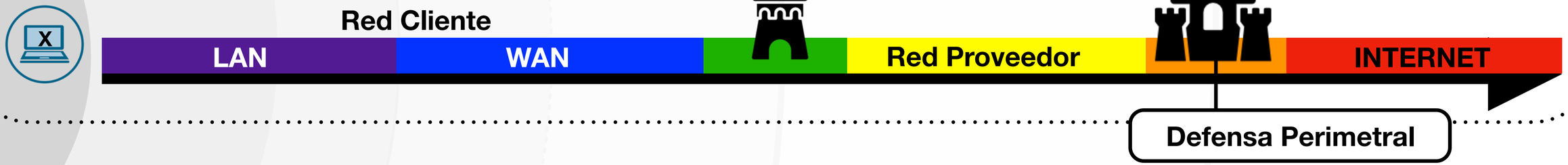
Vulnerabilidades en servidores

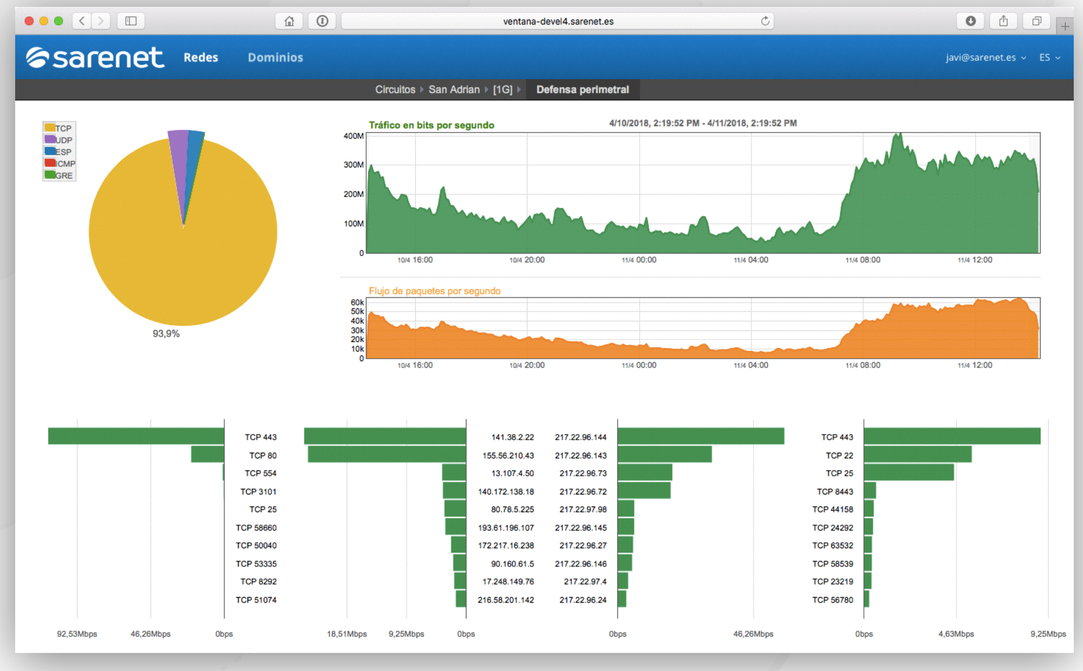
NAC Auth

SSL Portal

Gestión de los dispositivos NAC y control de accesos

Servicio de Seguridad Gestionada





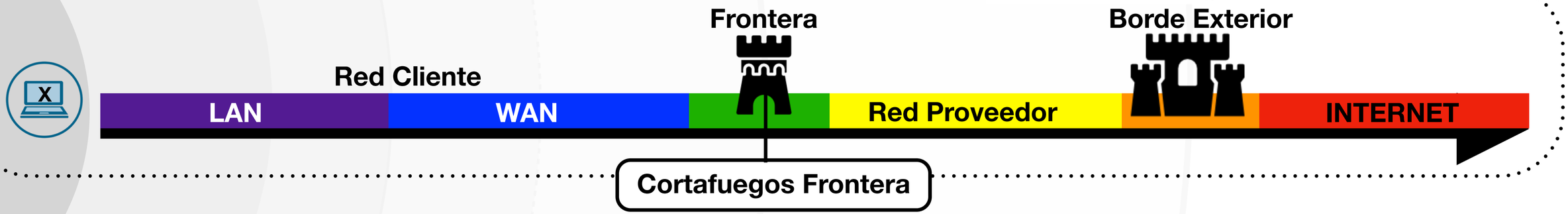
Aplicación Web

Gestión : cliente o Sarenet

Por IP o rango protegido

Desde **150 €/mes**

Servicio de Seguridad Gestionada



Alquiler y alojamiento de cortafuegos gestionado

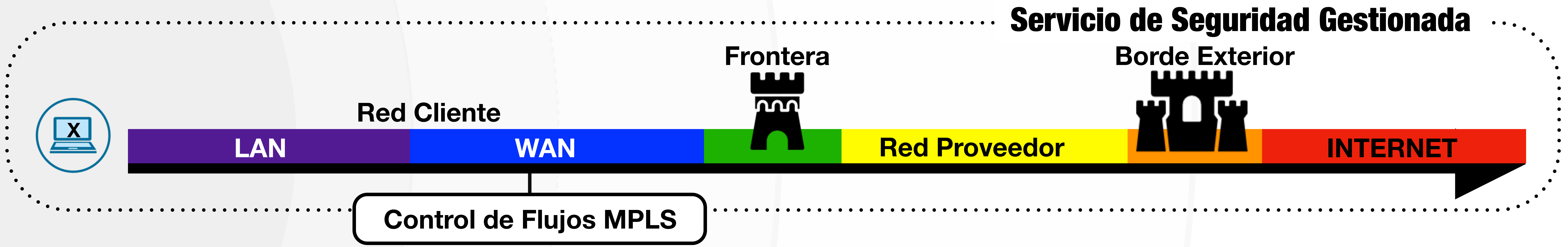
Actualizaciones del Firmware

Creación de las políticas de seguridad

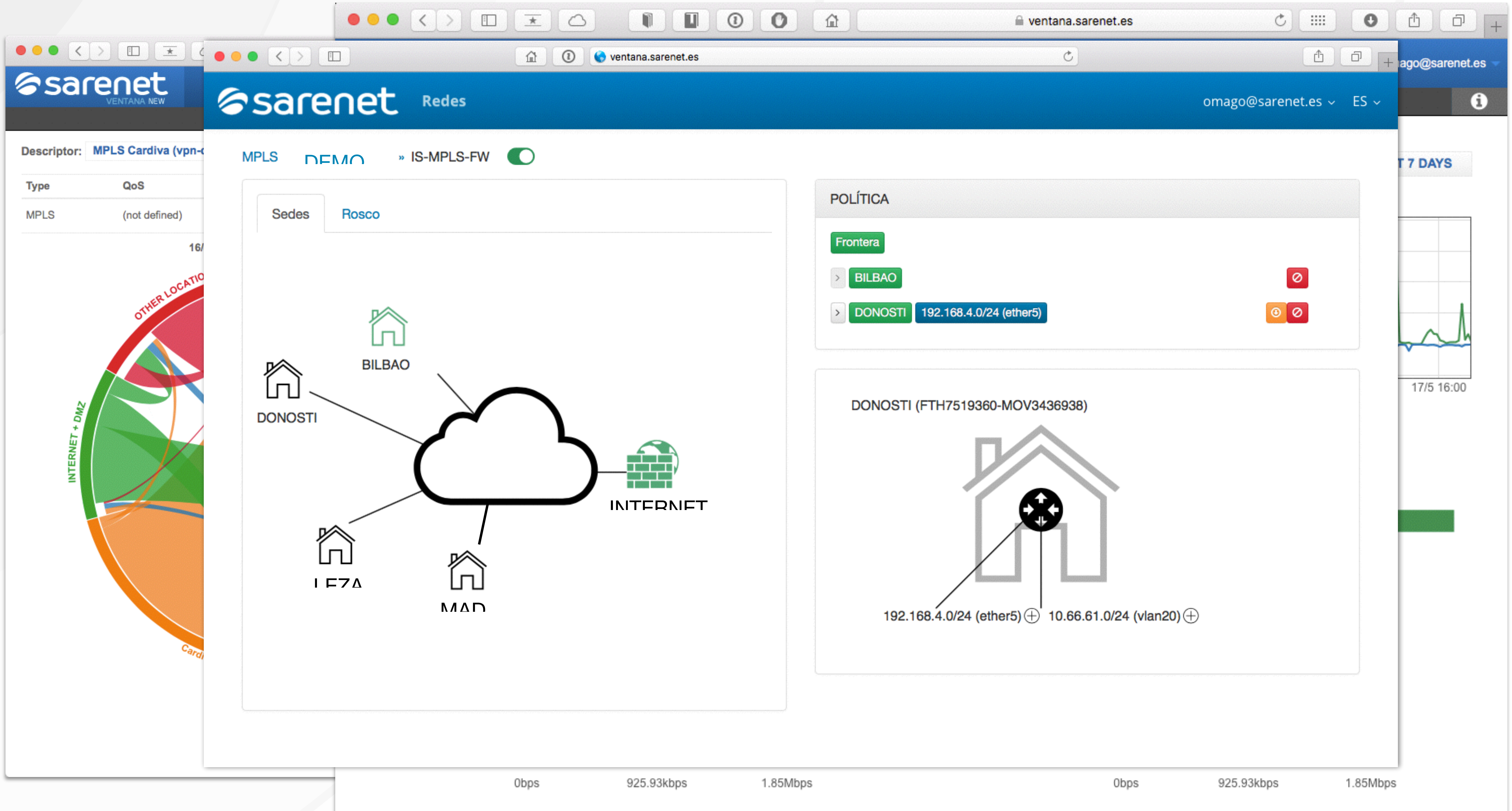
Gestión de accesos externos

Atención de las incidencias de seguridad : IPS/IDS, Botnets, virus

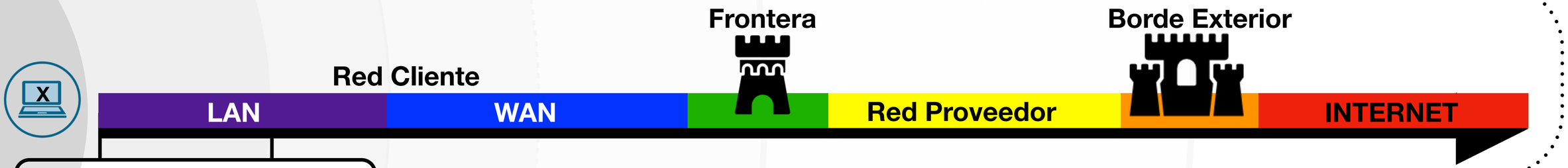
Gestión de sistemas de informes : fortianalyzer FAZ



Primer nivel … por sede

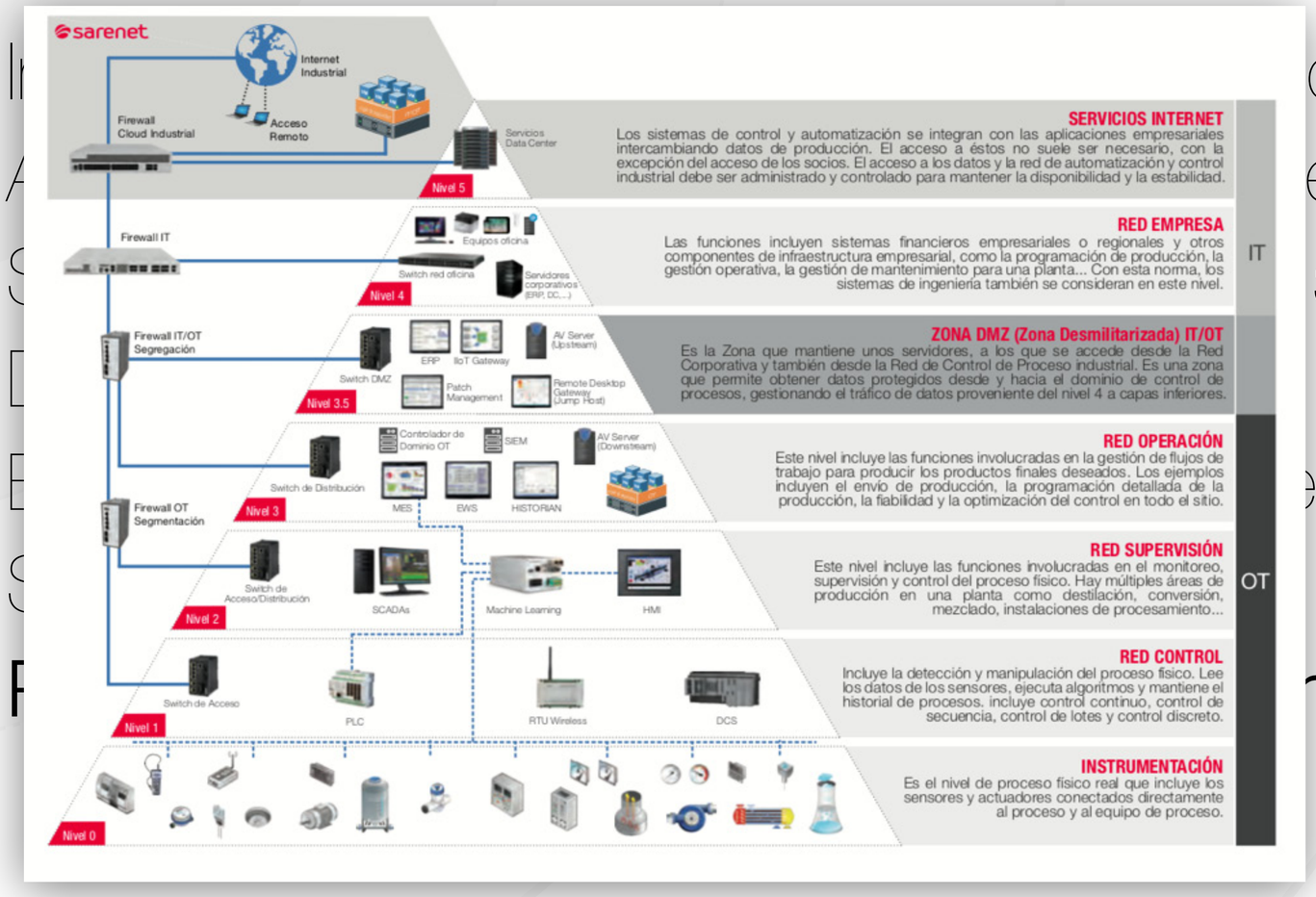


Servicio de Seguridad Gestionada



Segmentación LAN

Control de Acceso



NAC Auth

SSL Portal

Gestión de los dispositivos NAC y control de accesos

I de clien

A egmentar y segregar las redes

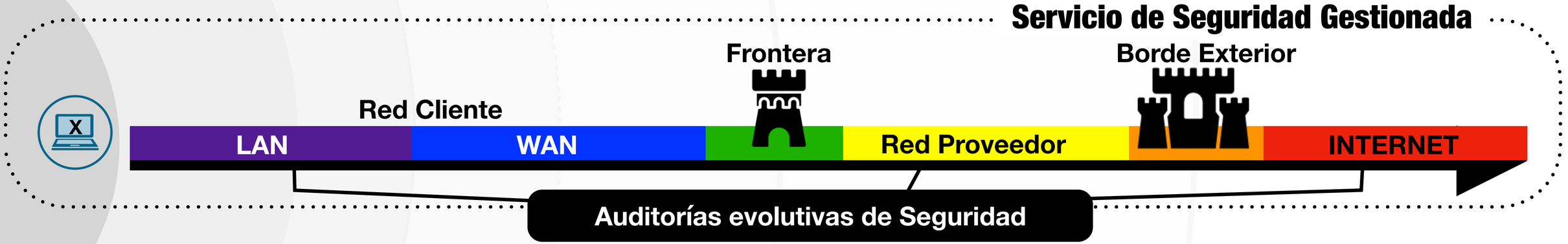
S switches y cortafuegos

E control de acceso a la LAN

S

R te poste

Gestión de redes Wifi



Contratación de la herramienta de auditoría evolutiva: 10 IPs, 500 €/año

Detección infraestructura crítica

Monitorización continua

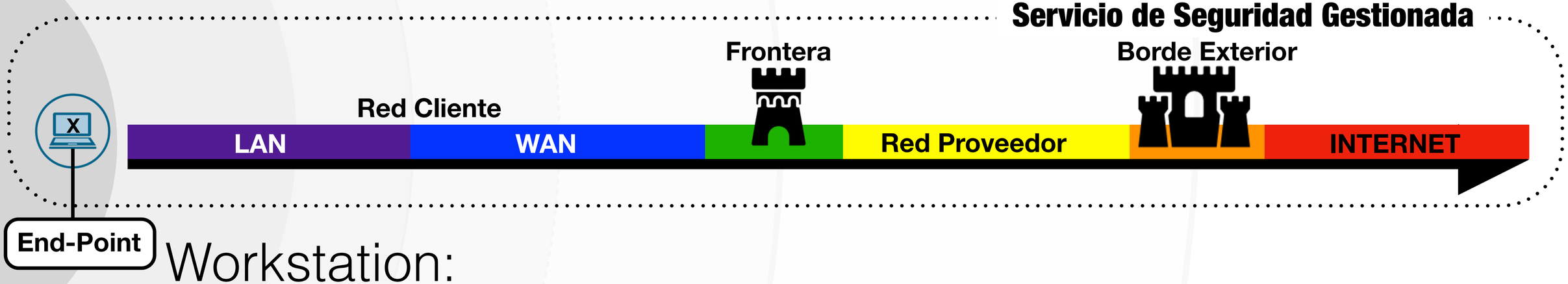
Soporte correctivo

- Alertas y vulnerabilidades

Soporte evolutivo

- Seguimiento continuo : reuniones periódicas y elaboración de informes con recomendaciones de acciones correctoras y de mejoras

Presupuestos a medida en base a fijo mensual : Desde 114 €/mes



Workstation:

Endpoint tradicional - 25 €/año
Intercept X - 35 €/año
Intercept X advanced con EDR - 70 €/año

Servers:

Central Server Protection - 59 €/año
Central Intercept X advanced - 120 €/año

Soporte en base a fijo mensual : Desde 57 €/mes

Plan de Contingencia

Sistemas Seguros de Almacenamiento **Veeam Cloud Connect**

Back-Up:

10€/mes por MV + espacio (ej.: 35€/mes -1TB)

Replication:

MV inactiva: 10€/mes + licencias de MS + almacenamiento

MV activa: 10€/mes + licencias de MS + almacenamiento + CPU + RAM

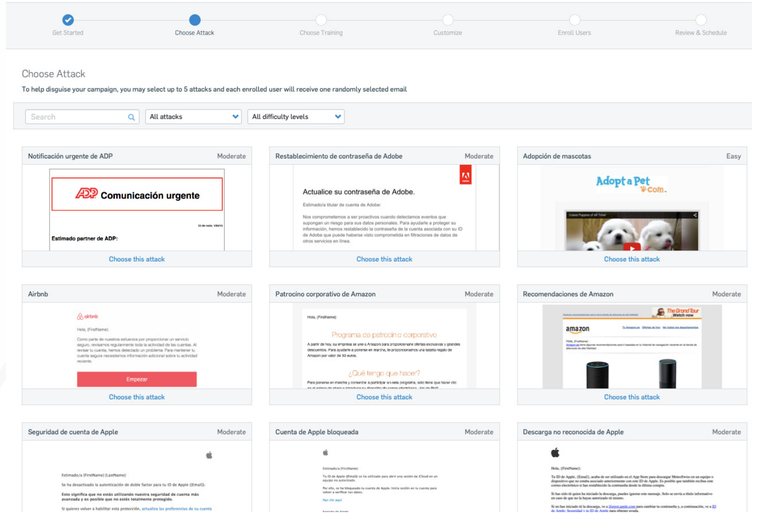
Failoverplan:

Estudio inicial + Costes de Replicación + IPs (10€/mes por IP)

Portal de concienciación: pishing

Alquiler de la herramienta : 100 usuarios, 19 €/año)
Soporte Sarenet : desde 57 €/mes

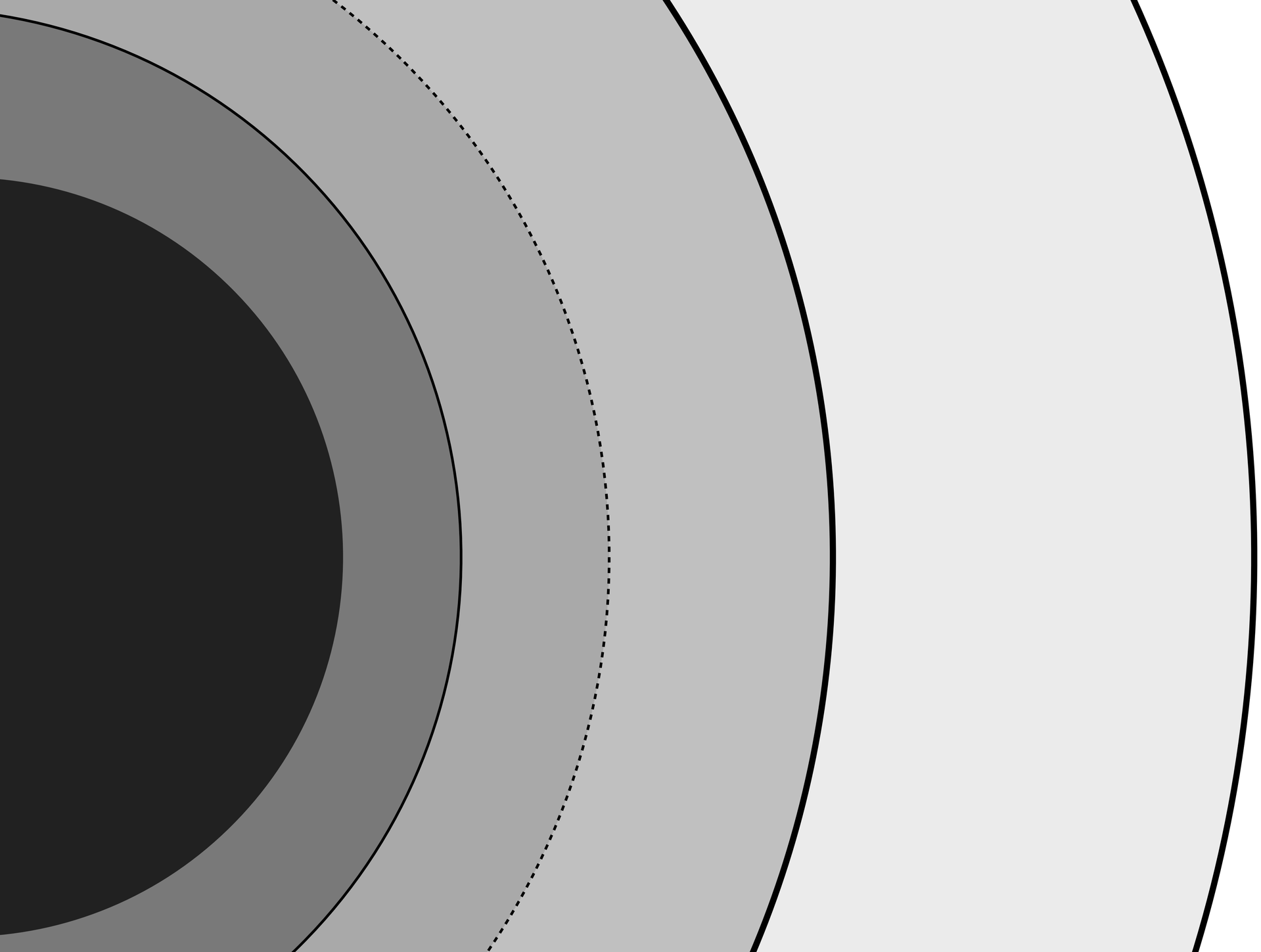
- Elaboración y análisis de campañas
- Reuniones de seguimiento e informes



SOC gestionado 24x7

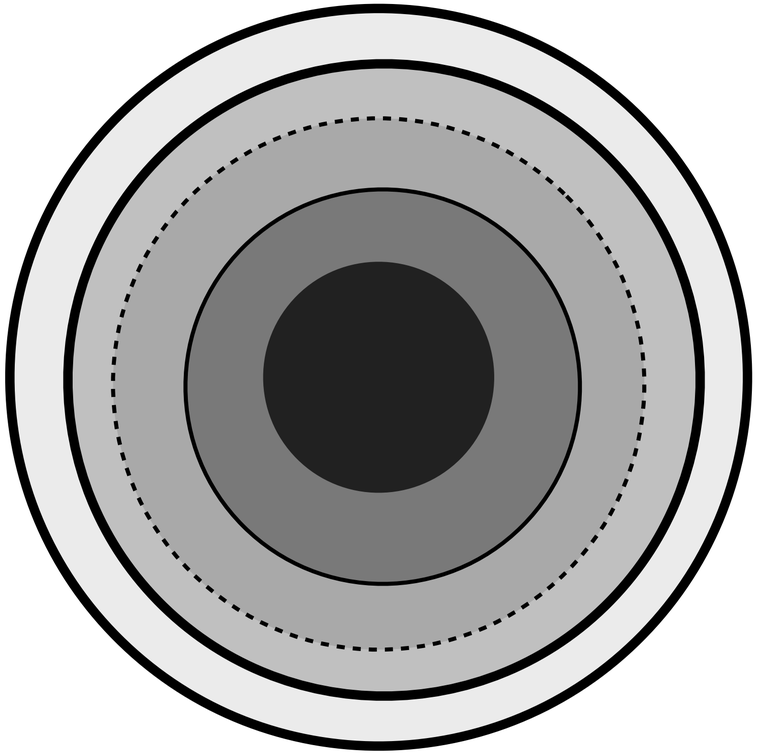
Security Center + SOC Sarenet

- Atención y comunicación de incidentes de seguridad.
- Administración de cambios en elementos de seguridad.
- Administración de respaldo de configuraciones
- Administratición y monitorización de eventos en cortafuegos y FAZ
- Monitorización de la red y de los equipos involucrados
- Monitorización de vulnerabilidades
- Hacking ético : test periódico de robustez de claves, simulación de ataques , etc..
- Generación mensual de informes ejecutivos
- SLA en base a tiempos de respuesta y calidad del soporte.



uridad Gestionada

Solución de seguridad integral
para nuestros clientes



¿Cómo empiezo a trabajar con Sarenet?


Los grandes viajes empiezan con un
simple paso,
puedes empezar haciéndonos
una simple consulta...

Patricia Ardines patricia@sarenet.es
Eduardo Arnedo eduardo.arnedo@sarenet.es
Pedro Xabier Alaña pedroxabier@sarenet.es
Aitor Jerez aitor@sarenet.es

Gràcies a tots