



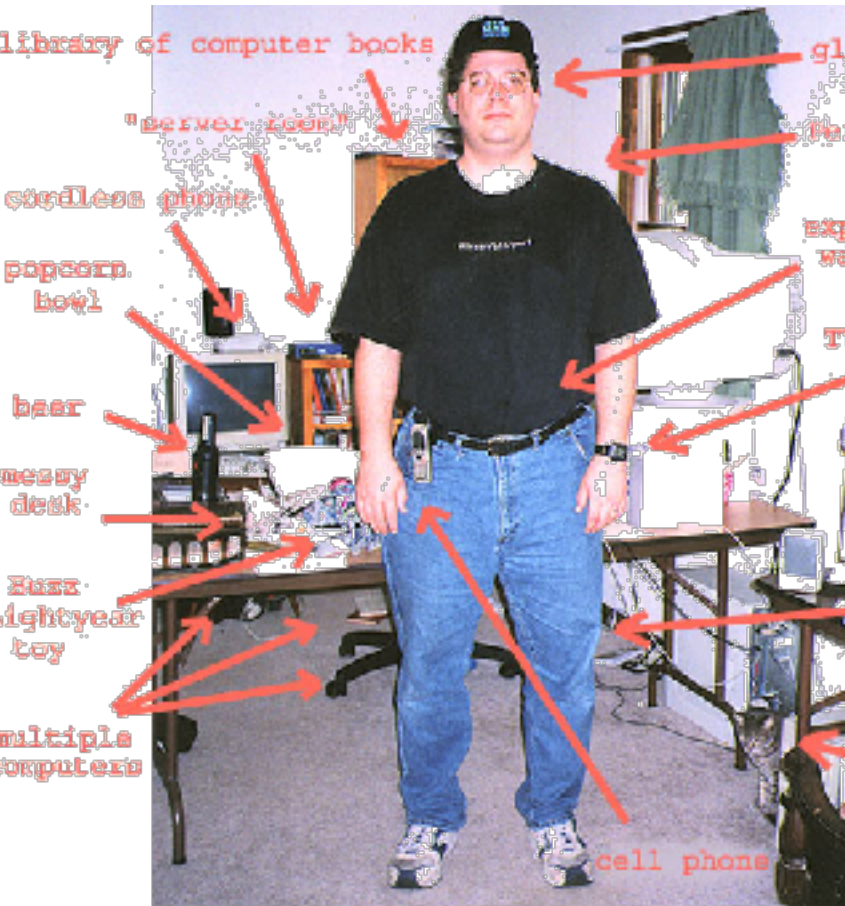
Consorti de
Serveis Universitaris
de Catalunya

Mitigación de ataques DDoS en la Anella Científica

Maria Isabel Gandía Carriedo
19º Foro ESNOG
CSUC – CATNIX, 6-4-2017



¿Quiénes somos y de dónde venimos?



Edgy short haircut, often dyed red or black

Quirky-cool reading glasses on a chain around her neck or perched on end of her nose.

High neckline and cardigans

Dorky-chic dangly earrings

expanding waistline

TV remote/watch

his "good" pants

Hemline no shorter than knee-length

cat

Sensible flats



STYLE ICON

Annie Potts in Ghostbusters



(c) 2002 Jen Hilton

CSUC

Consorci de
Serveis Universitaris
de Catalunya

¿Qué hacemos?

CSUC

ConSORCI de
Serveis Universitaris
de Catalunya

Comunicaciones

Promoción

**Administración
Electrónica**

**Cálculo
Científico**

Bibliotecas

**Portales y
Repositorios**

**ConSORCIACIÓN de
Servicios y
Compras Conjuntas**

**Operaciones y
Seguridad**



Y en Comunicaciones, ¿qué hacemos?



- ✓ Red académica de Catalunya
- ✓ 82 instituciones conectadas (universidades, centros de investigación...)
- ✓ AS13041
- ✓ Conectada a RedIRIS y al CATNIX
 - ✓ 2 nodos troncales
 - ✓ Anchos de banda de 2 Mbps a 20 Gbps



- ✓ Punto neutro de internet en Catalunya
- ✓ 32 entidades conectadas (operadores, proveedores de servicios, de contenido...)
- ✓ AS49638 (para servicios)
- ✓ Otros AS conectados para servicios (root servers F, J, K y L, etc).



DDoS: La tostadora nos ataca

LA VANGUARDIA

Tecnología

Aplicaciones | Electrónica | Innovación | Internet | Móviles y Dispositivos | Redes sociales | Trucos | Videjuegos

AVANCE: "El BSC y el BSO se dan dos meses para evitar la ruptura" en la portada de este martes

Así se grave

Twitter queda inaccesible por un ataque informático

DOS VECES EN UN DÍA

Un ciberataque masivo a EEL a grandes webs

Twitter, Airbnb, Netflix y el 'New York Times', entre las informadas

Los hackers vigilan

ABC Tecnología

OTROS populares sitios web también se ven afectados

Titulares: Las seis noticias que debes leer antes de irte a dormir

Tecnología | Redes

Twitter, Spotify, Netflix y otras plataformas quedan inutilizadas por un ciberataque

» Un proveedor de DNS estadounidense ha sufrido un ataque desde países

» Aumenta la psicosis contra los hackers en EEUU, que han

Twitter fue dejada de funcionar como consecuencia de un ataque de hackers (Chris Ruffolo / Flickr)

✓ Ataque basado en Mirai, dirigido desde IoT

✓ **Volumétrico (en bits/s o paquetes/s):**

- Satura el ancho de banda disponible.
- Objetivo: la infraestructura.
- Fuerza bruta. Hay que pararlo “aguas arriba”.
- Pueden ser detectados por los gestores de la red.

✓ **Tablas de estado:**

- Satura las tablas del Firewall/IDS/Balanceador.
- Objetivo: la infraestructura.
- Fuerza bruta. Hay que pararlo “aguas arriba”.
- No detectables a priori.

✓ **Aplicación:**

- Satura los recursos del servidor de aplicaciones.
- Su objetivo son servicios específicos.
- Parecen tráfico legítimo para los gestores de la red.
- Utilizan vulnerabilidades de la aplicación.

Una mezcla de todos

Según dicen los expertos...

- ✓ Los objetivos de los ataques son (Q4 2016):
 - 49% empresas TI (45% en Q2)
 - 32% sector público (14%)
 - 7% bancos y servicios financieros (23%)
- ✓ El pico de tráfico ha aumentado un 63% en un año
- ✓ El 86% de los ataques emplea múltiples métodos

Fuente: <http://www.verisign.com/assets/infographic-ddos-trends-Q42016.pdf>

- ✓ Ataque promedio, 931 Mbps (1,2 Gbps a finales de 2017)
- ✓ El más grave, de 800 Gbps (un 60% mayor que en 2015)
- ✓ 88% de los ataques < 2 Gbps
- ✓ 91% duran < 1 hora

Fuente: Arbor, 12th Worldwide Infrastructure security report

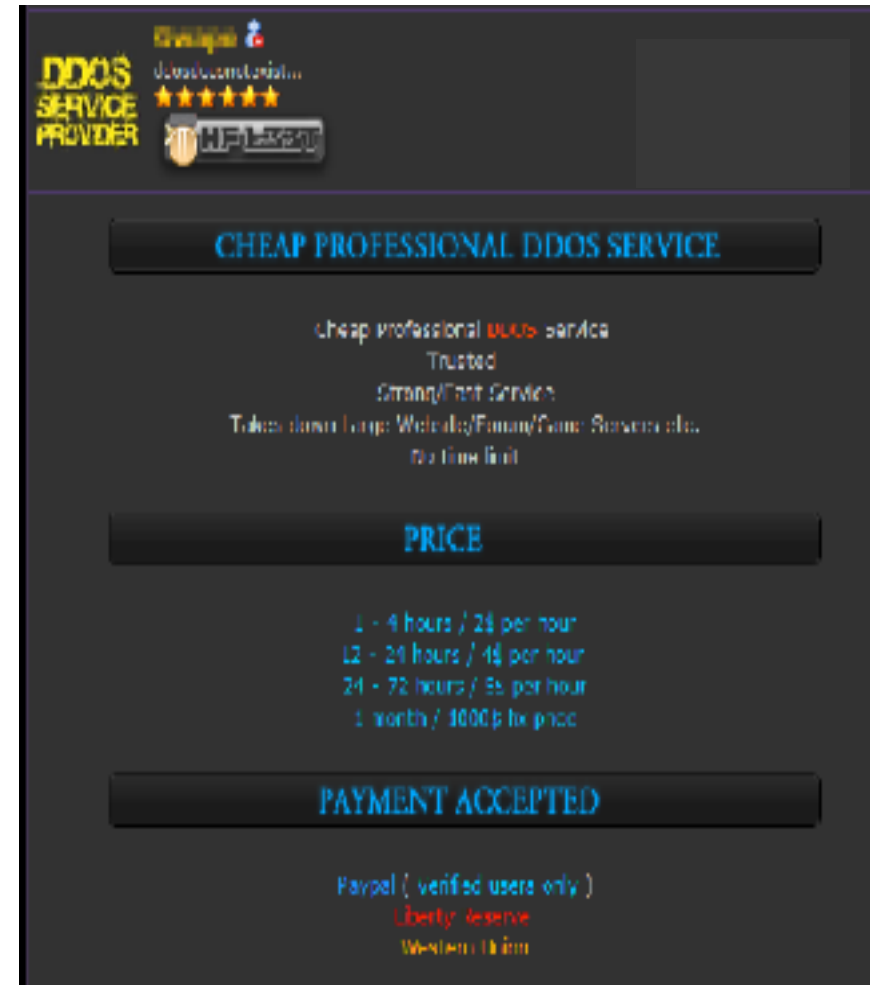
¿Y en una universidad o centro de investigación?

✓ ¿Por qué?

- Evitar un examen
- Investigación
- Vandalismo
- *Gamers*
- Motivos políticos
- Represalias a máquinas infectadas
- Maniobra de distracción
- Es facilísimo

✓ ¿Cómo?

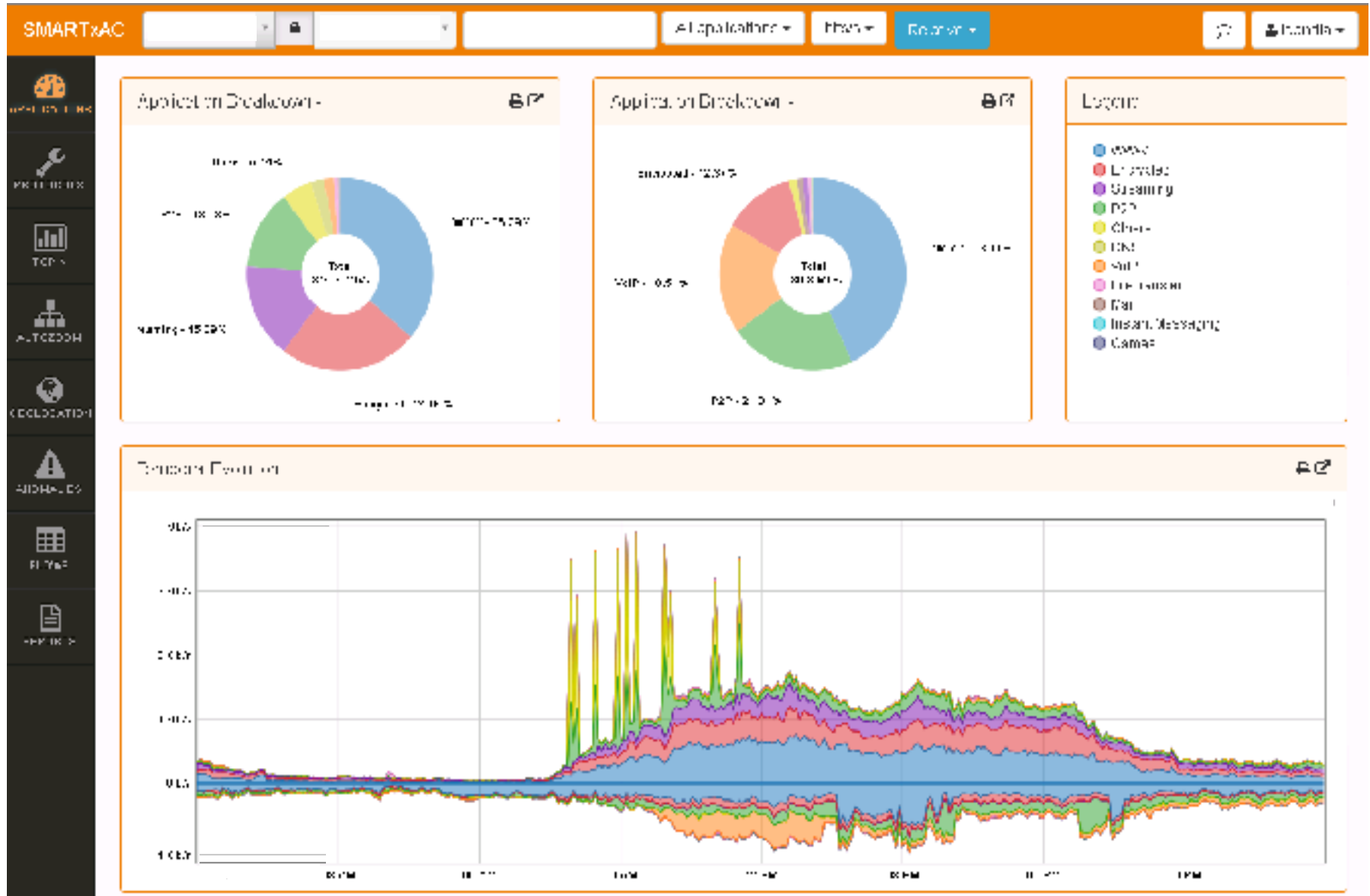
- DDoSaaS



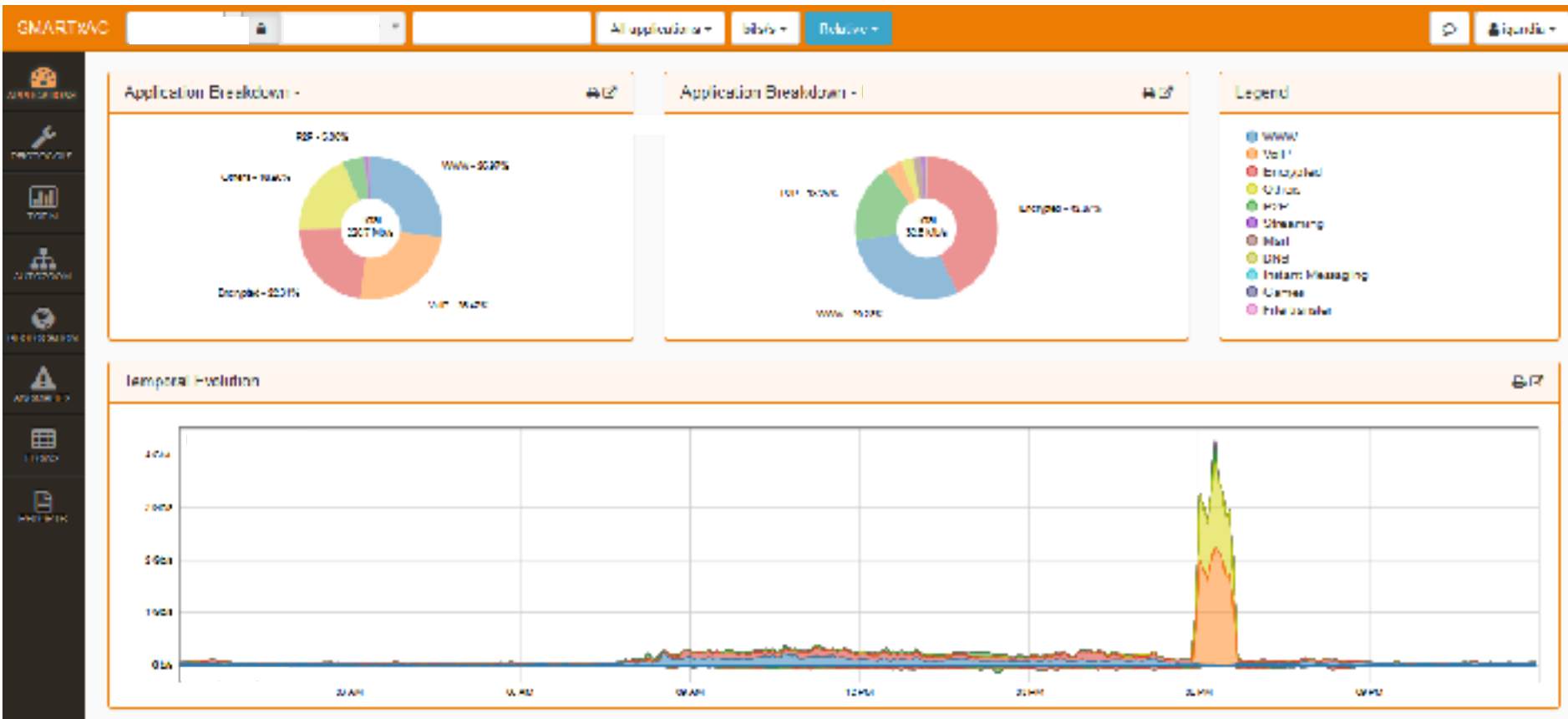
The image shows a screenshot of a website for a DDoSaaS service. At the top left, there is a logo that says "DDoS SERVICE PROVIDER" in yellow and red. To its right, there is a "Gigamon" logo and a "Trustpilot.com" rating of 5 stars. Below the logo, there is a "CHEAP PROFESSIONAL DDOS SERVICE" button. Underneath, the text reads: "Cheap professional ddos service", "Trusted Strong/Fast Service", and "Takes down Large Website/E-mail/Game Servers etc. No time limit". Below this is a "PRICE" button, followed by a list of pricing options: "L1 - 4 hours / 24 per hour", "L2 - 24 hours / 48 per hour", "24 - 72 hours / 96 per hour", and "1 month / 1000 per price". At the bottom, there is a "PAYMENT ACCEPTED" button, followed by the text: "Paypal (verified users only)", "Liberty reserve", and "Western Union".

El origen puede estar dentro, aunque el ataque venga de fuera

Ataques volumétricos a una universidad con 10 Gbps

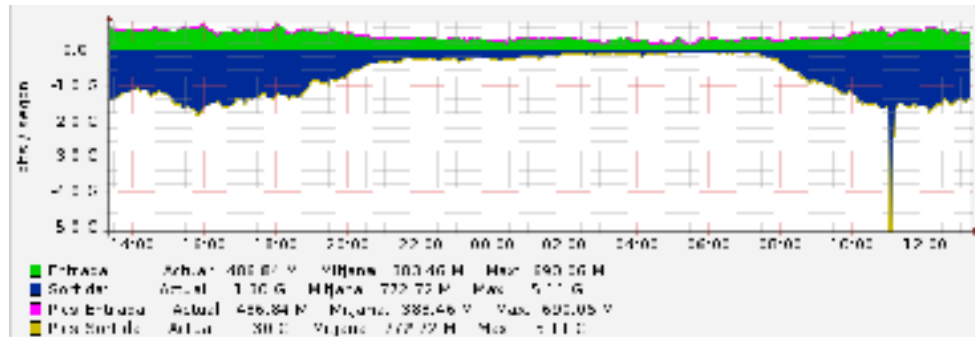


Ataque volumétrico a una universidad con 1 Gbps

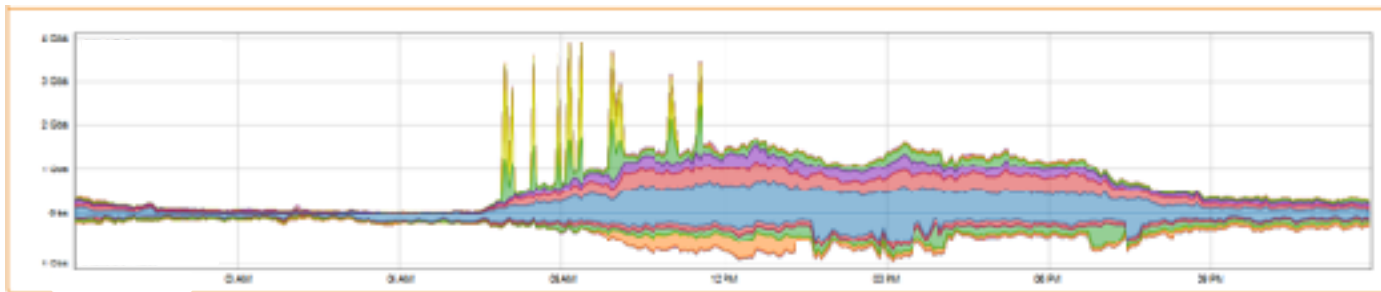


Distintas vistas de ataques

✓ Cacti (SNMP)



✓ SMARTxAC (Netflow)

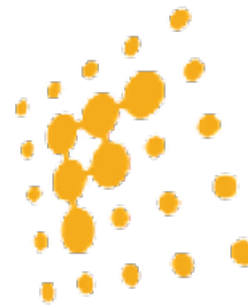


✓ Team Cymru Flow sonar (Netflow)

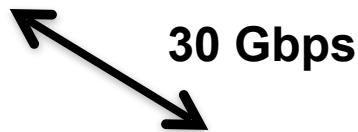
timestamp	count	src ip	src port	dst ip	dst port	protocol	alert source	type
2016-11-15 16:48:47	1	*	39152	1	25	6	ip reputation	proxy
2016-11-15 16:48:46	1	*	31339		80	6	ip reputation	conficker
2016-11-15 16:48:41	3	*	37781		80	6	ip reputation	conficker
2016-11-15 16:48:39	1	*	3128		61966	6	ip reputation	proxy
2016-11-15 16:48:36	1	*	40268		23	6	ip reputation	conficker
2016-11-15 16:48:32	27	*	443	*	4414	6	ip reputation	conficker
2016-11-15 16:48:28	2	*	80	*	11100	4	ip reputation	conficker



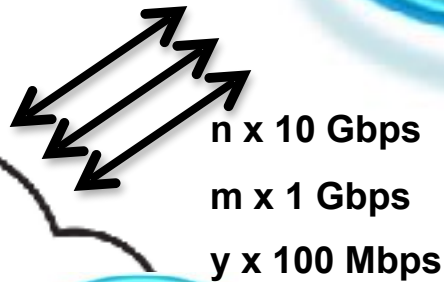
Red **IRIS**



CATNIX



**ANELLA
CIENTÍFICA**

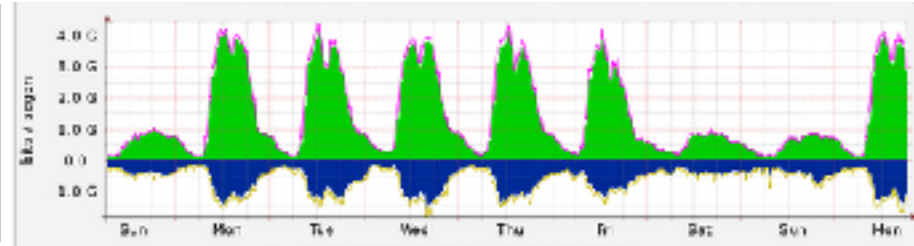
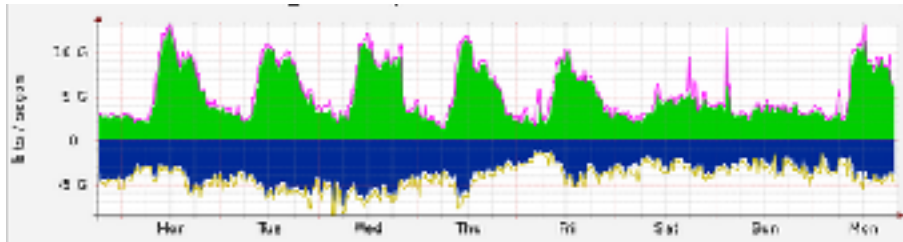


**ANELLA
CIENTÍFICA** ...



**Proveedor
comercial**

El tráfico regular a nivel IPv4



85 % de internet,
(634644 rutas)
70% del tráfico

30 Gbps

10 Gbps

16 % de internet
(100409 rutas)
30% del tráfico

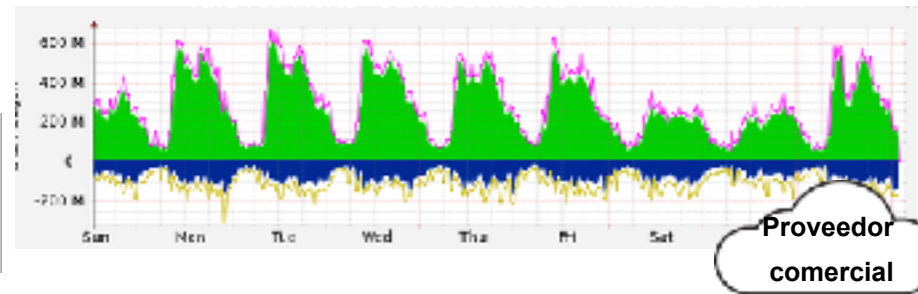
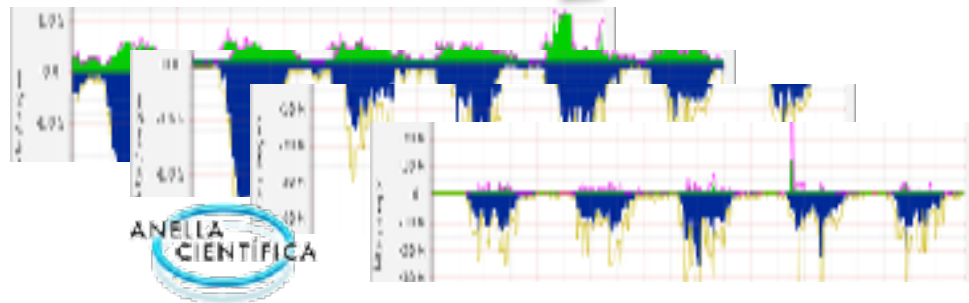
**ANELLA
CIENTÍFICA**

0,00002 % de internet

10 Gbps

10 Gbps

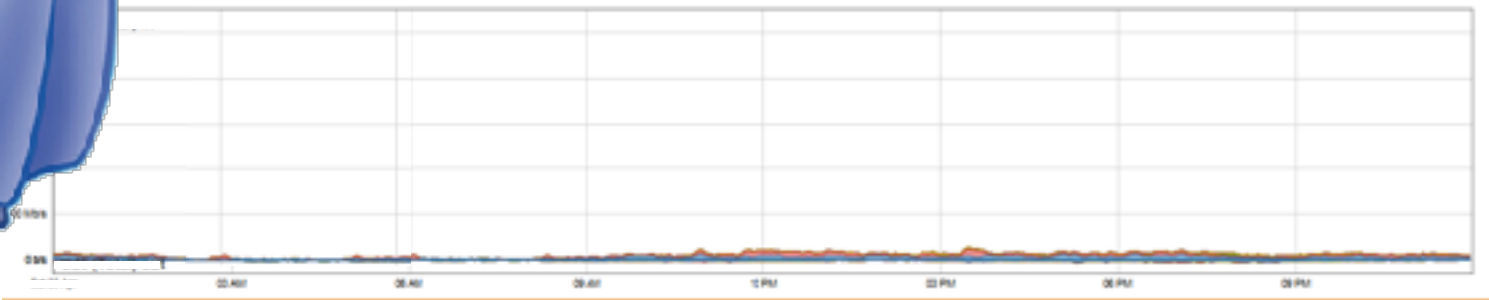
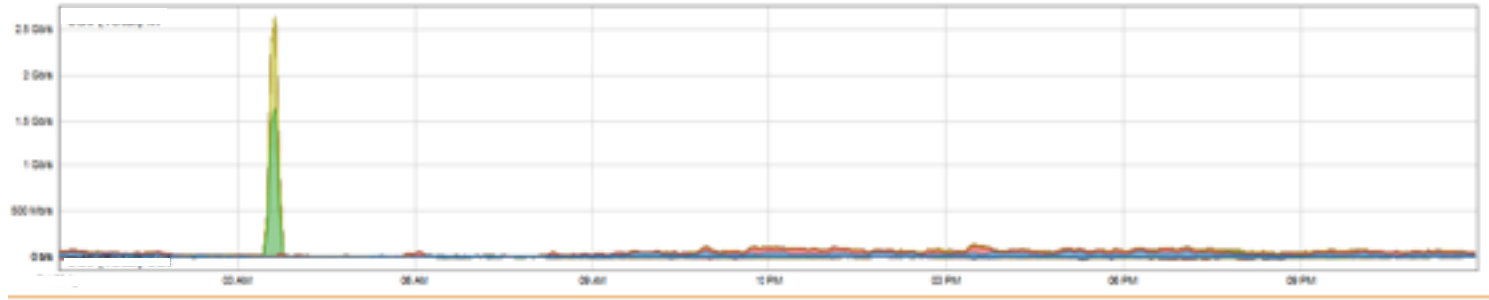
85 % de internet



¿Por qué en la Anella Científica?

- ✓ En una encuesta sobre nuevos servicios, **un 95%** de miembros consideró necesaria una plataforma de mitigación de ataques DDoS (4,67 sobre 5).
- ✓ Las universidades, preocupadas por los resultados de un ataque durante su proceso de matrícula.
- ✓ Se habían detectado ataques de más de 5 Gbps.
- ✓ Necesario mitigar en 24x7.
- ✓ El precio de adquisición de las plataformas de mitigación de DDoS es elevado => Adquirirlas y utilizarlas de forma conjunta desde el CSUC.

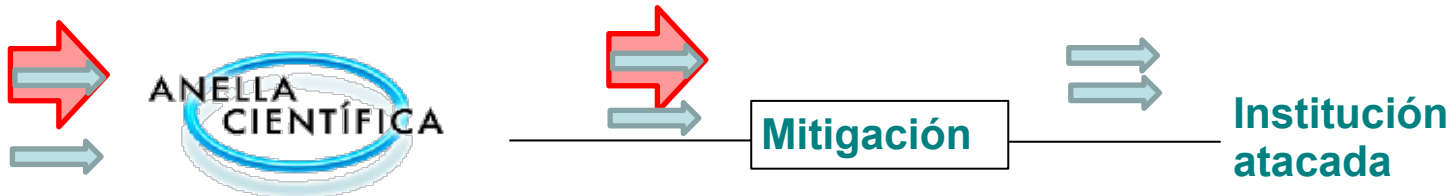
¿Tan fácil es mitigar un ataque?



Dos pruebas de concepto

✓ Se realizaron dos PoC o *testbeds*:

A Solución en línea con capacidad 10 Gbps:



B Solución fuera de línea con capacidad 10 Gbps

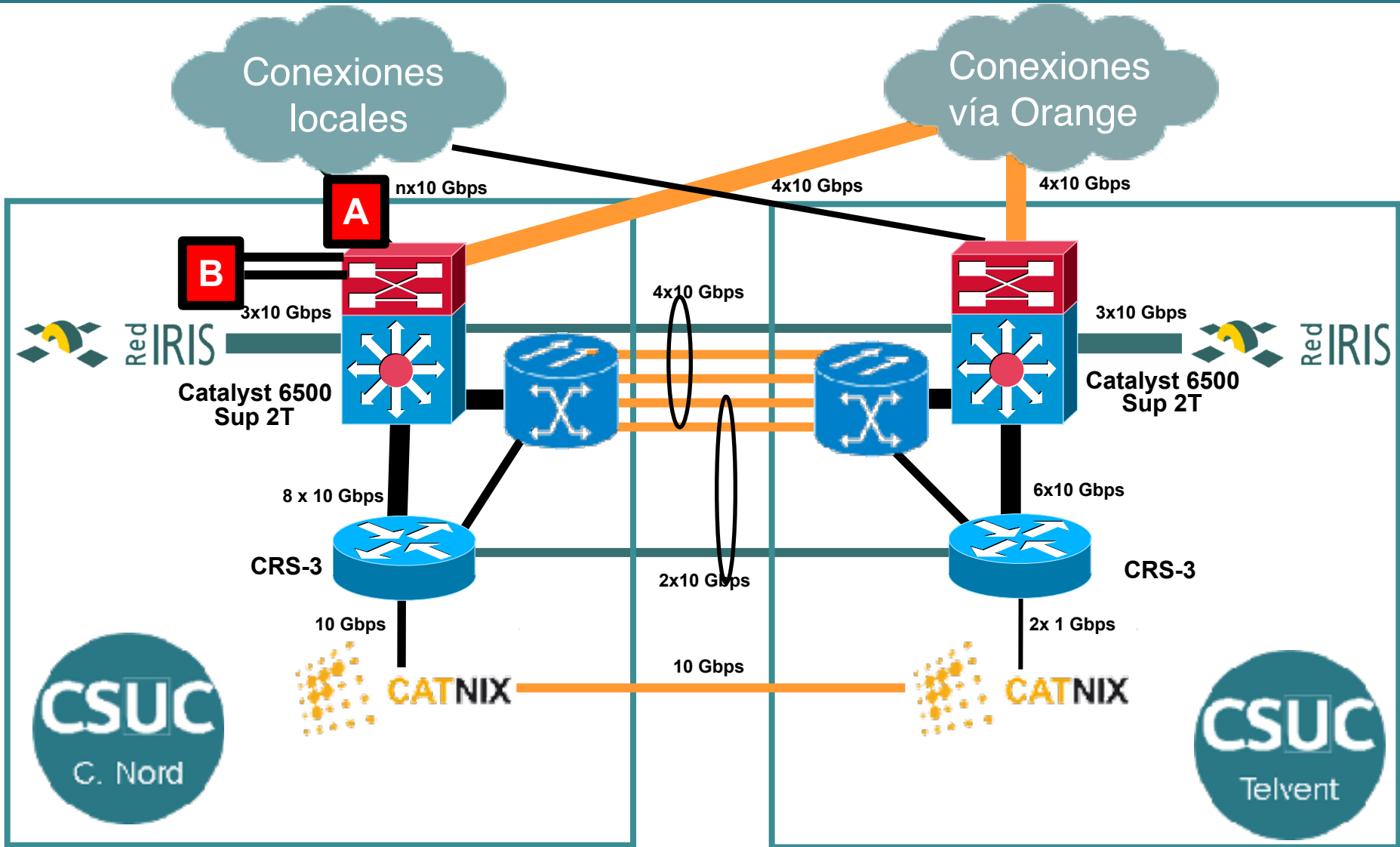


✓ PoCs en marcha durante el periodo de matrícula de las universidades

- ✓ Para la puesta en marcha de las PoC, informaron de:
 - Rangos de las universidades
 - Direcciones IP o rangos a proteger con mayor granularidad
 - Una dirección IP señuelo con la que hacer pruebas
 - Personas autorizadas a solicitar mitigaciones
 - Si se prefería mitigación manual o automática

- ✓ Una vez hechas las pruebas, valoraron las dos soluciones.
- ✓ Decidieron qué tipo de plataforma se ajustaba mejor a sus necesidades.

Topología física de la Anella Científica (sólo tráfico regular)

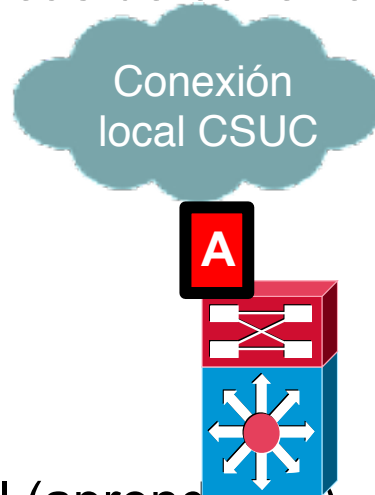


— Conexiones vía RedIRIS

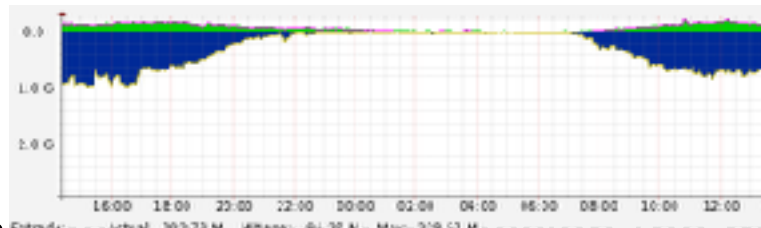
— Conexiones vía Orange

— Conexiones locales

✓ Se activó en una de las líneas de conexión del CSUC, 10 Gbps.



✓ Se entrenó con tráfico real (aprendizaje).

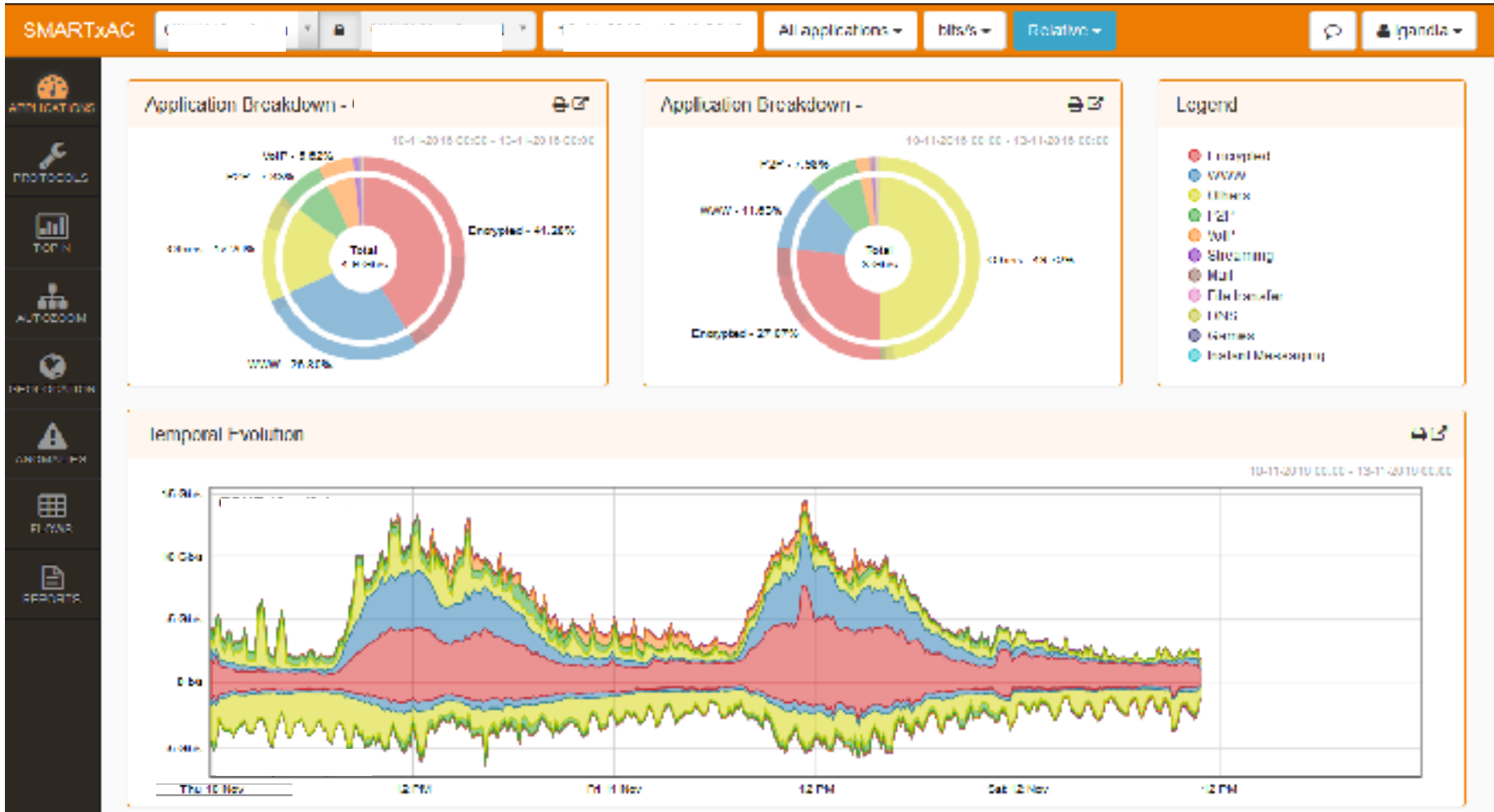


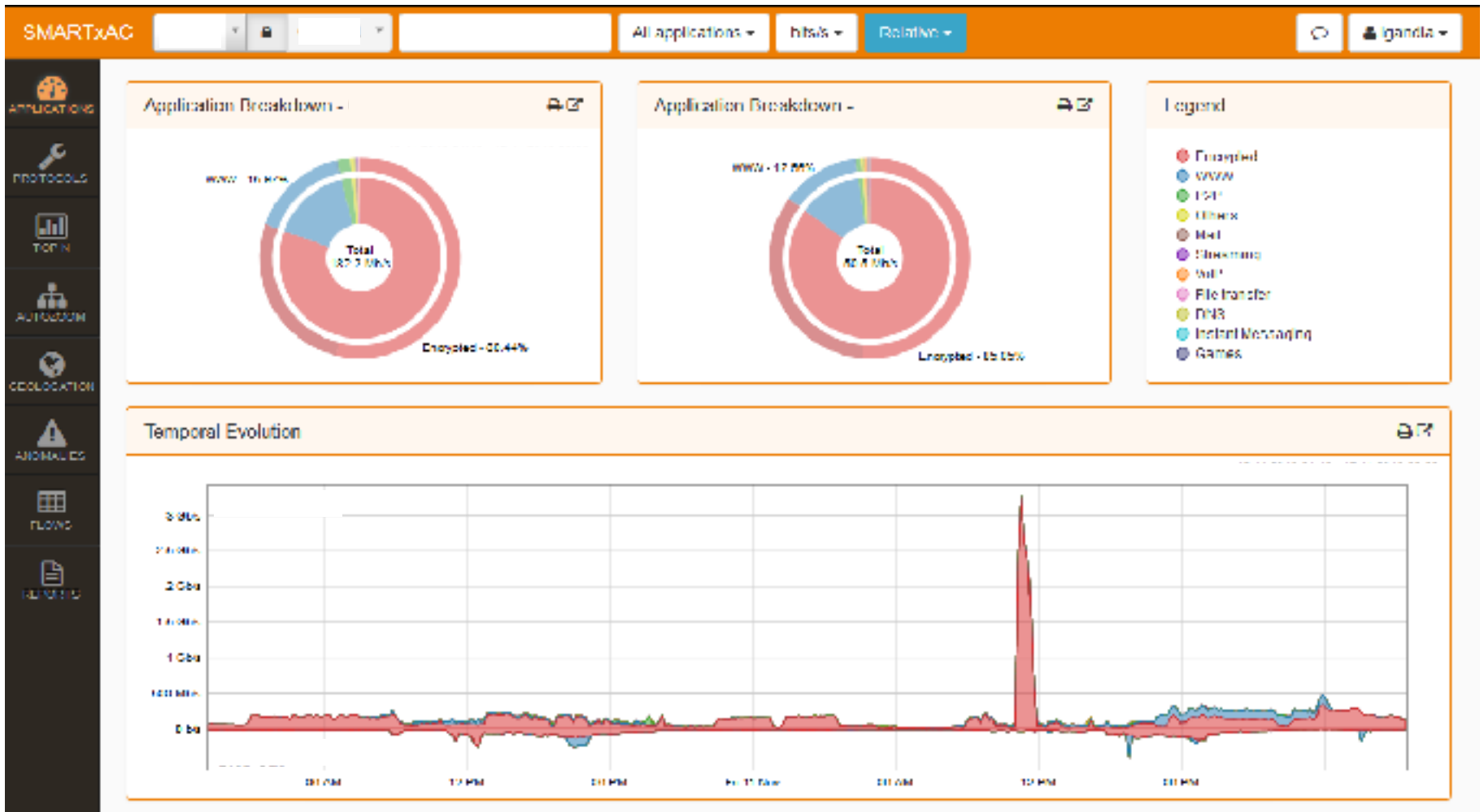
✓ Posteriormente, se dejó en modo detección (no mitigación).

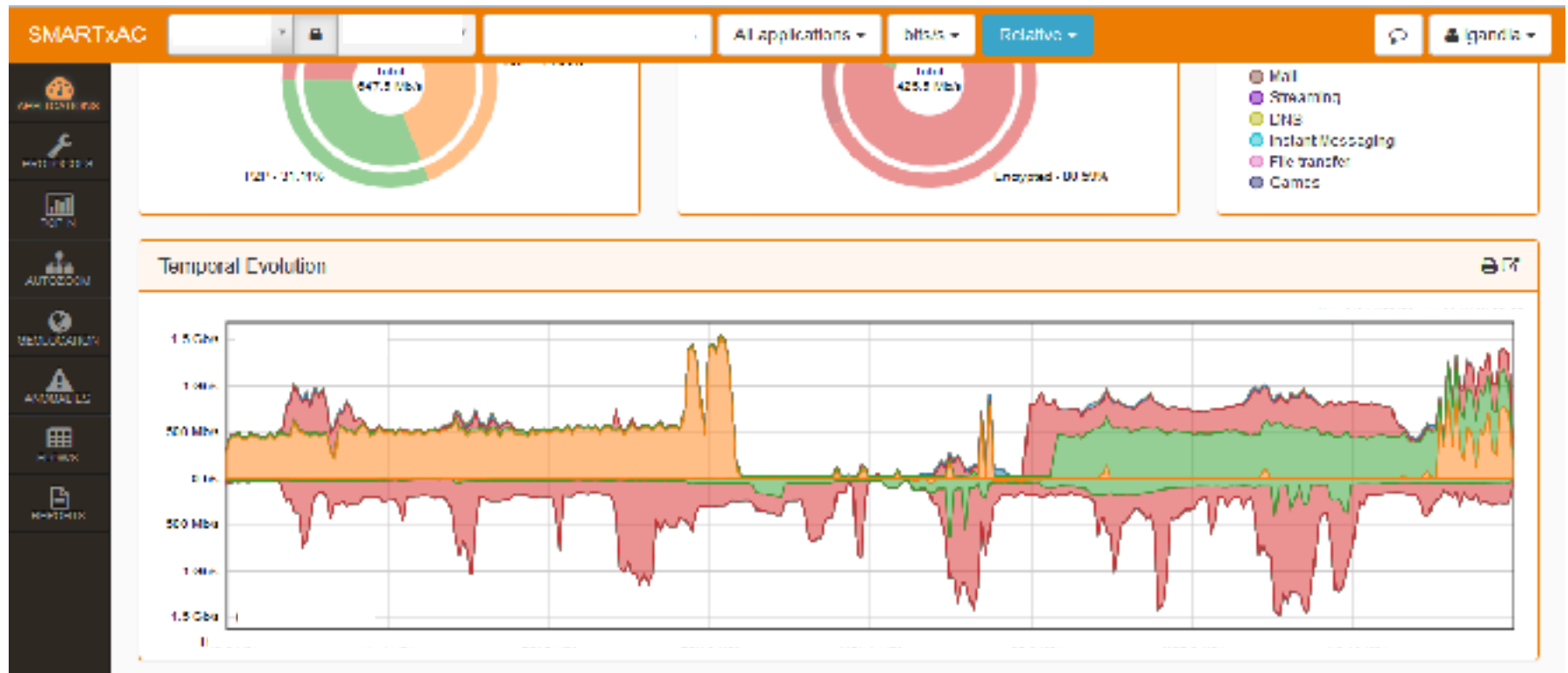
✓ Se observó cuál hubiese sido el comportamiento en caso de haber estado en modo mitigación

✓ **Tráfico legítimo de supercomputación detectado como ataque.**

El tráfico de investigación no sigue patrones estándar

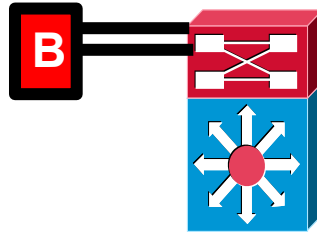






B Plataforma fuera de línea

- ✓ Se activó para las universidades, 2 interfaces 10 Gbps:

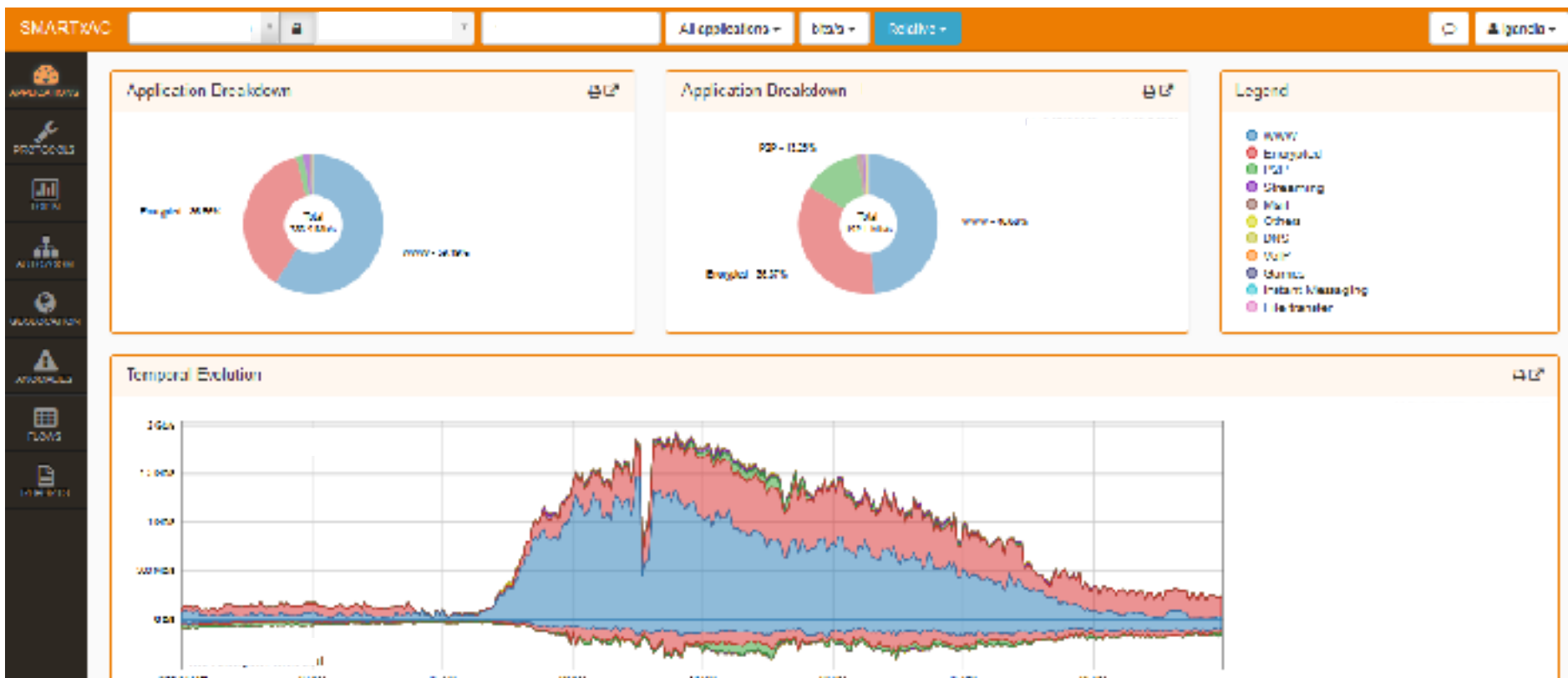


- ✓ Objetos diferenciados para global de la universidad, matrícula y DNS.
- ✓ Se entrenó con tráfico real de los DNS del CSUC (aprendizaje).



- ✓ Se probó con direcciones señuelo con distintas mitigaciones.
- ✓ Posteriormente, se observaron las alertas.
- ✓ **Falsos positivos cuando el perfil cambia brúscamente.**
- ✓ Y se mitigó en entorno real a petición de una universidad, sin una alerta grave asociada.

La primera mitigación en la práctica: mitigando zombies





- ✓ Mitigación automática rápida, prácticamente no requiere intervención manual.
- ✓ Muy útil en entornos de *hosting* (*web*, *DNS*), con perfiles más estables que los de una red académica.
- ✓ Al pasar todo el tráfico a través del equipo, detecta hasta los ataques más pequeños.
- ✓ Interfaz de gestión sencilla.
- ✓ Permite bypass físico.
- ✓ Puede revisar el tráfico en ambos sentidos.



- ✓ Con el perfil poco estándar de nuestro tráfico, las mitigaciones automáticas son peligrosas.
- ✓ Al ser una “caja” en medio de la red, tiene los peligros derivados de un mal funcionamiento.
- ✓ Poca granularidad de perfiles (8) dada la diversidad de patrones de tráfico.
- ✓ No escala cuando crece la red o bien hay que añadir elementos adicionales (puntos adicionales de fallo).
- ✓ Poca granularidad en las estadísticas.



- ✓ Solución basada en la red
- ✓ No interfiere con el resto del tráfico, sólo se desvía el que va hacia la IP atacada.
- ✓ Un fallo en equipo de mitigación no afecta a la red
- ✓ Es válido para el tráfico de los dos nodos, mediante configuración de los routers.
- ✓ Es escalable sin añadir más “cajas”.
- ✓ Granularidad en el número de objetos gestionados y en las estadísticas.



- ✓ Arquitectura compleja, especialmente en el caso de la Anella Científica, con VRF existentes.
- ✓ Mayor coste económico que la solución en línea.
- ✓ Necesita dos elementos físicos para detectar y mitigar.
- ✓ Se basa en muestreo de paquetes, no analiza el 100% del tráfico.
- ✓ Requiere actualización de firmas.

✓ Solución fuera de línea basada en Arbor:

✓ SP-7000:

- Portal de la solución
- Monitoriza tanto el router como el TMS
- Recibe full-routing del router y anuncia rutas atacadas hacia el TMS

✓ TMS-2800:

- Recibe el tráfico atacado para aplicar reglas de mitigación
- Devuelve el tráfico “limpio”
- Mitigación inicial 10 Gbps
- Capaz de mitigar hasta 40 Gbps (30 Mpps).

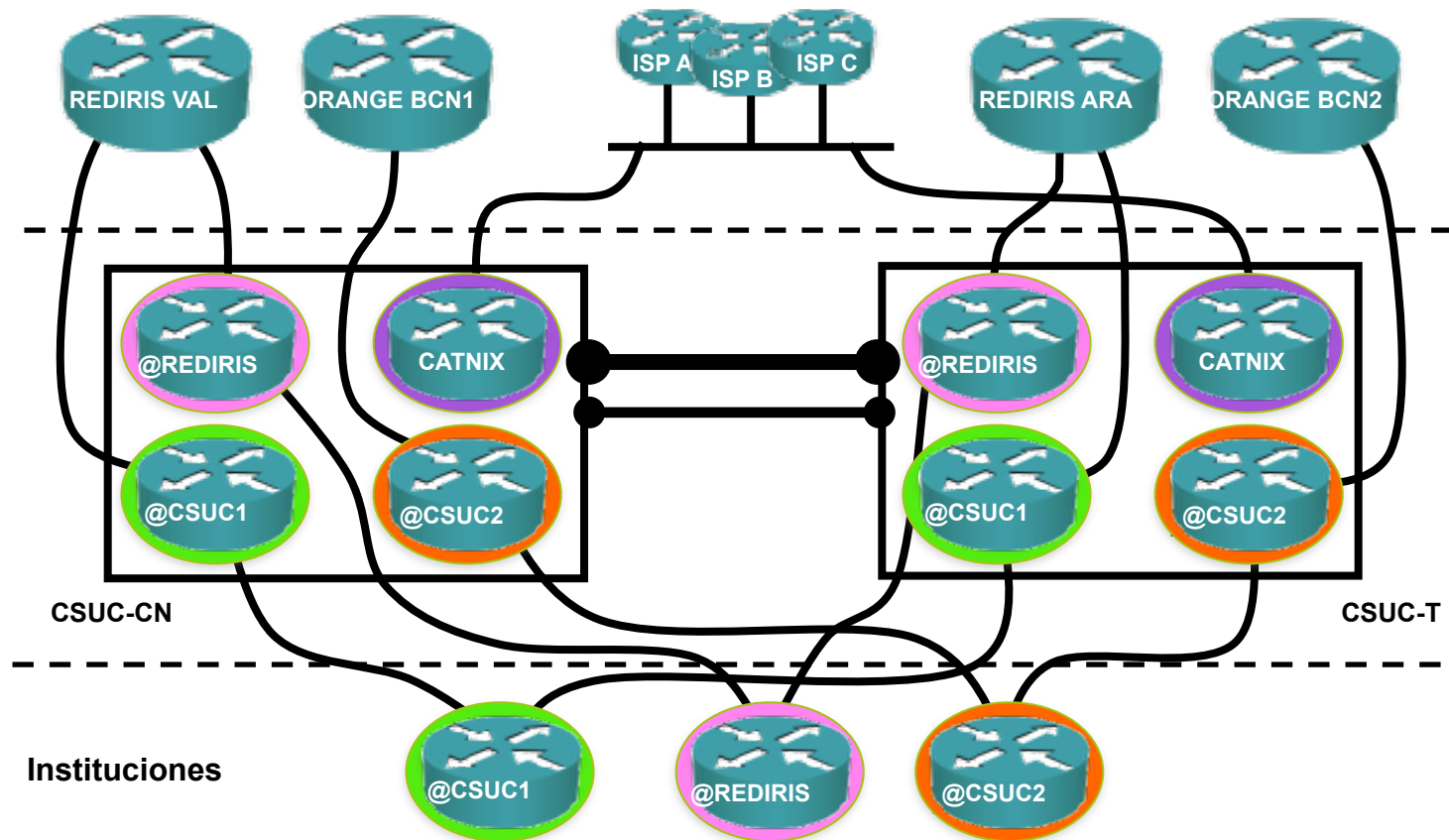
✓ Sistema basado en SNMP, Netflow y BGP.

✓ Permite detectar, mitigar y generar informes de tráfico por aplicación, de alertas y mitigaciones.

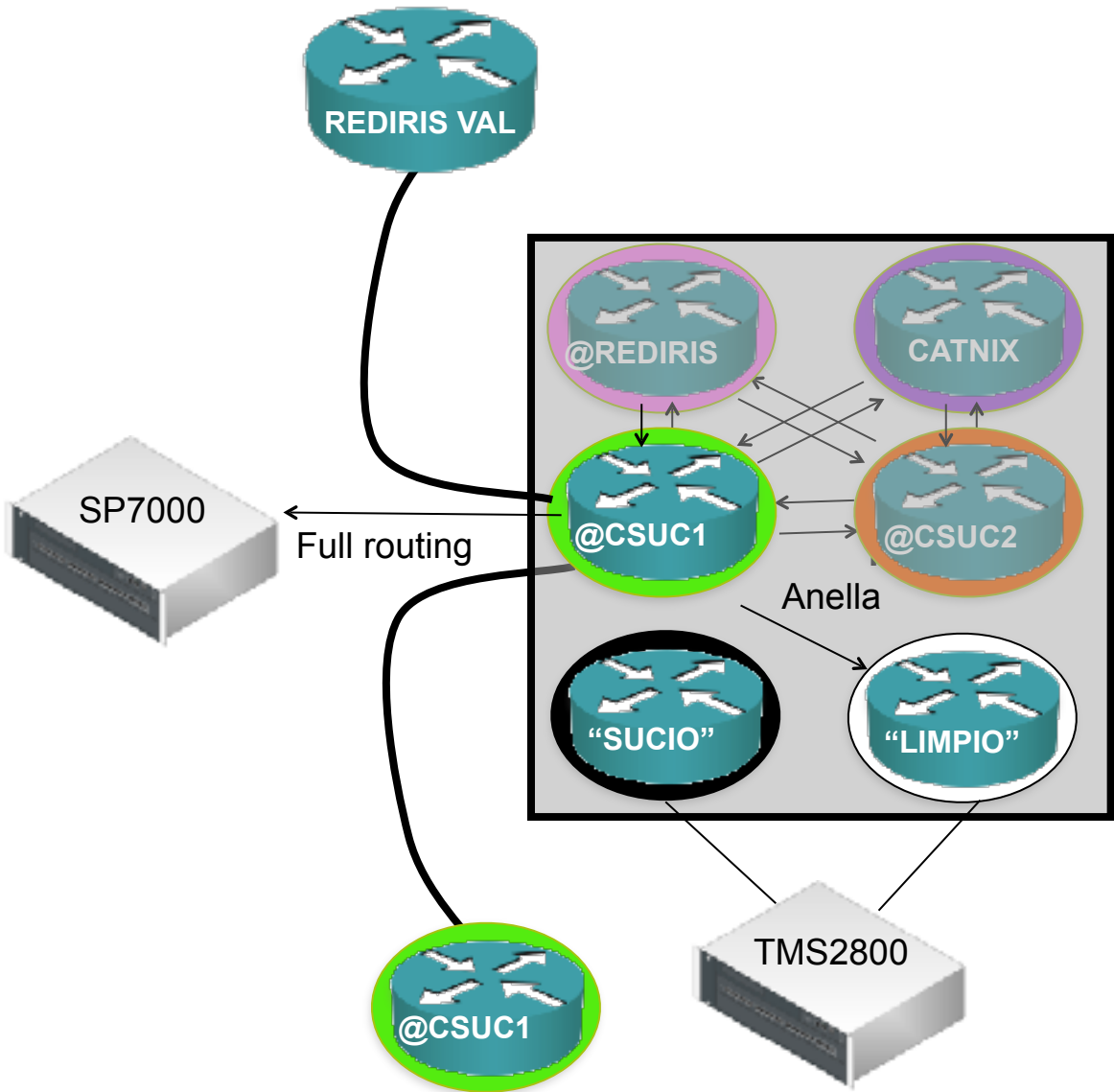
Rediseño de la arquitectura

- ✓ La Anella Científica ya contenía VRF => Nuevas políticas para nuevos VRF de tráfico limpio y sucio en cada nodo + integración con BFD.
- ✓ Flujos Netflow desde los routers a plataforma SMARTxAC => Desde plataforma SMARTxAC a equipo detección.

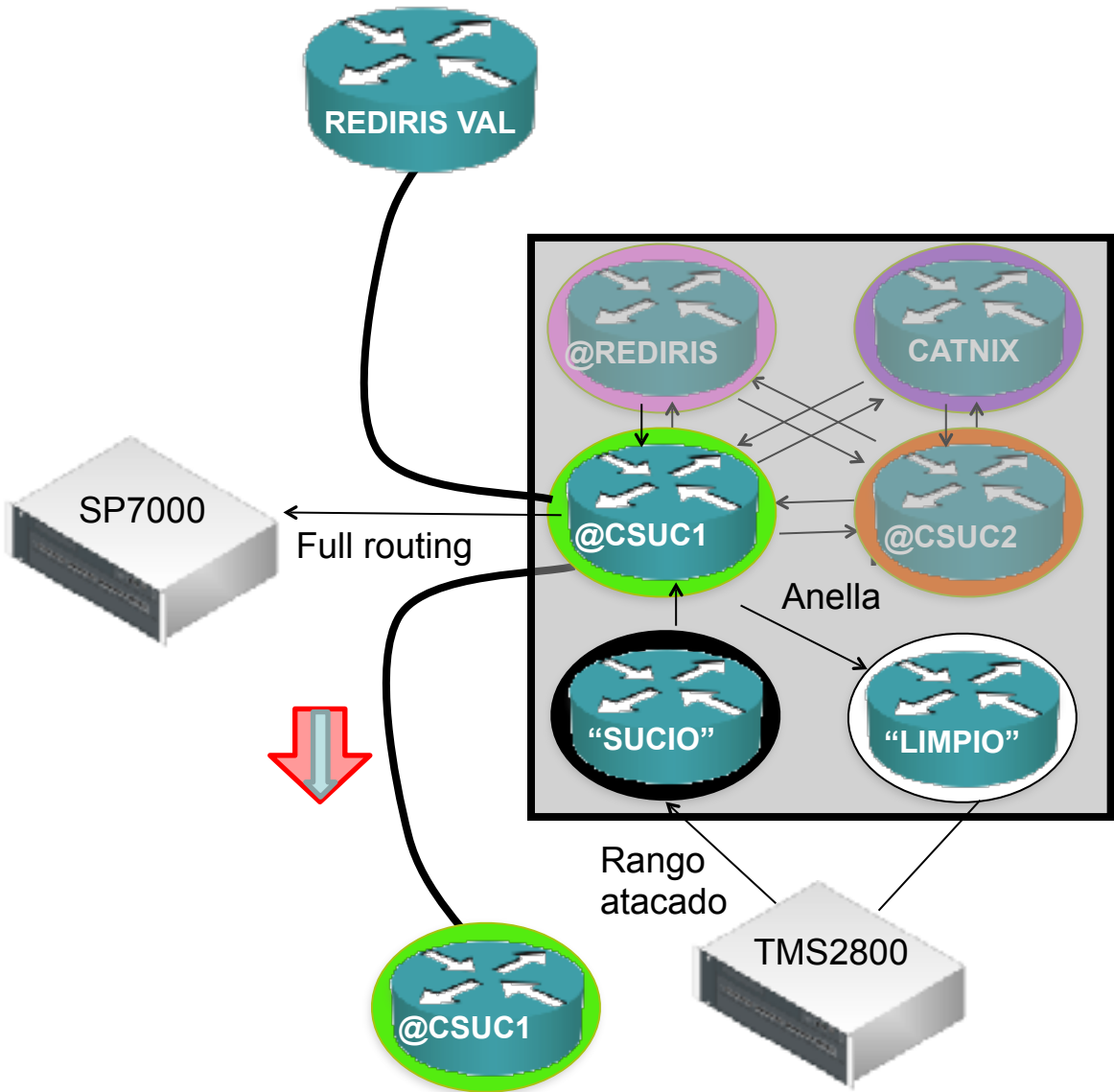
Tránsito y peerings



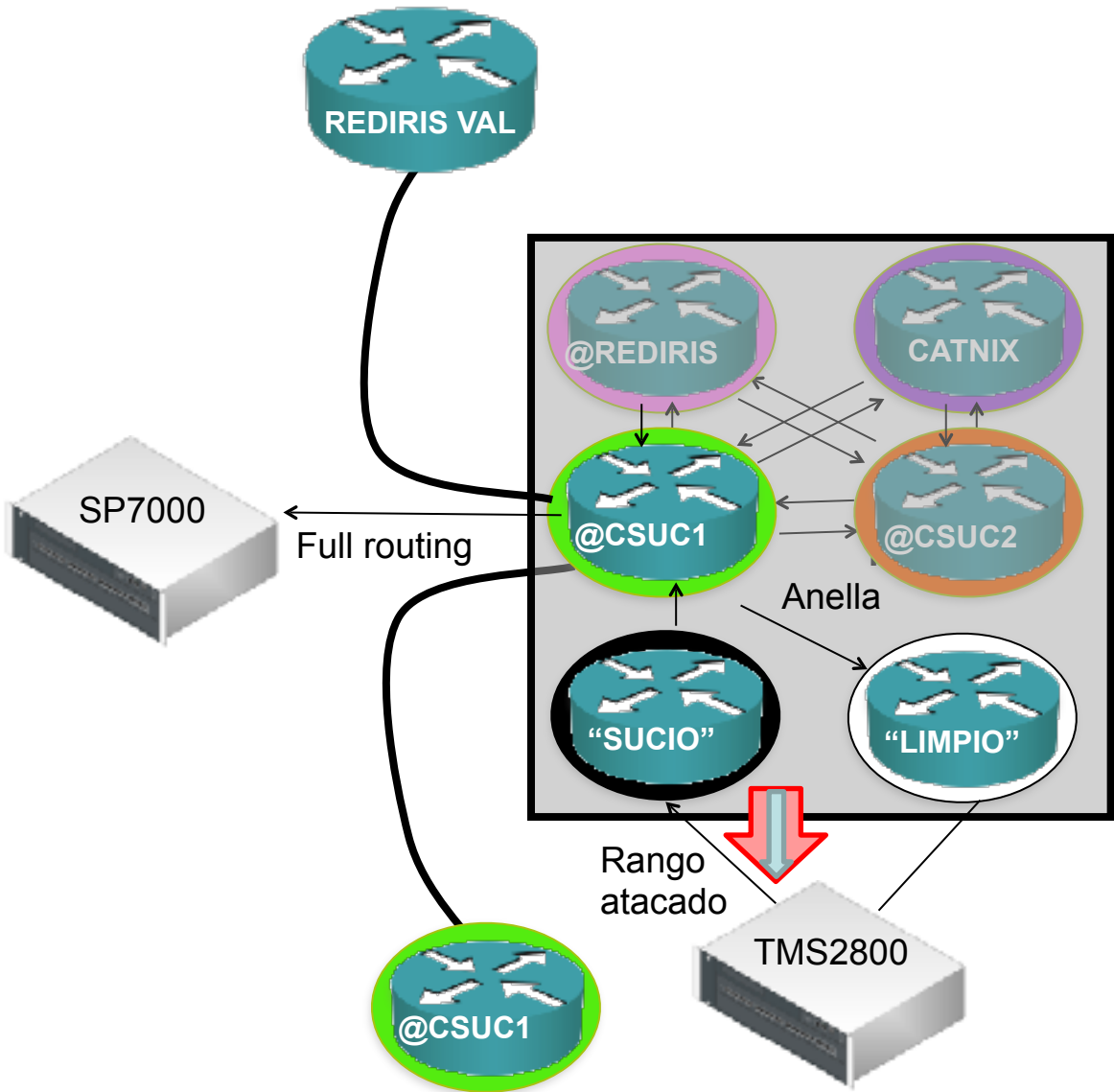
Rediseño de la arquitectura



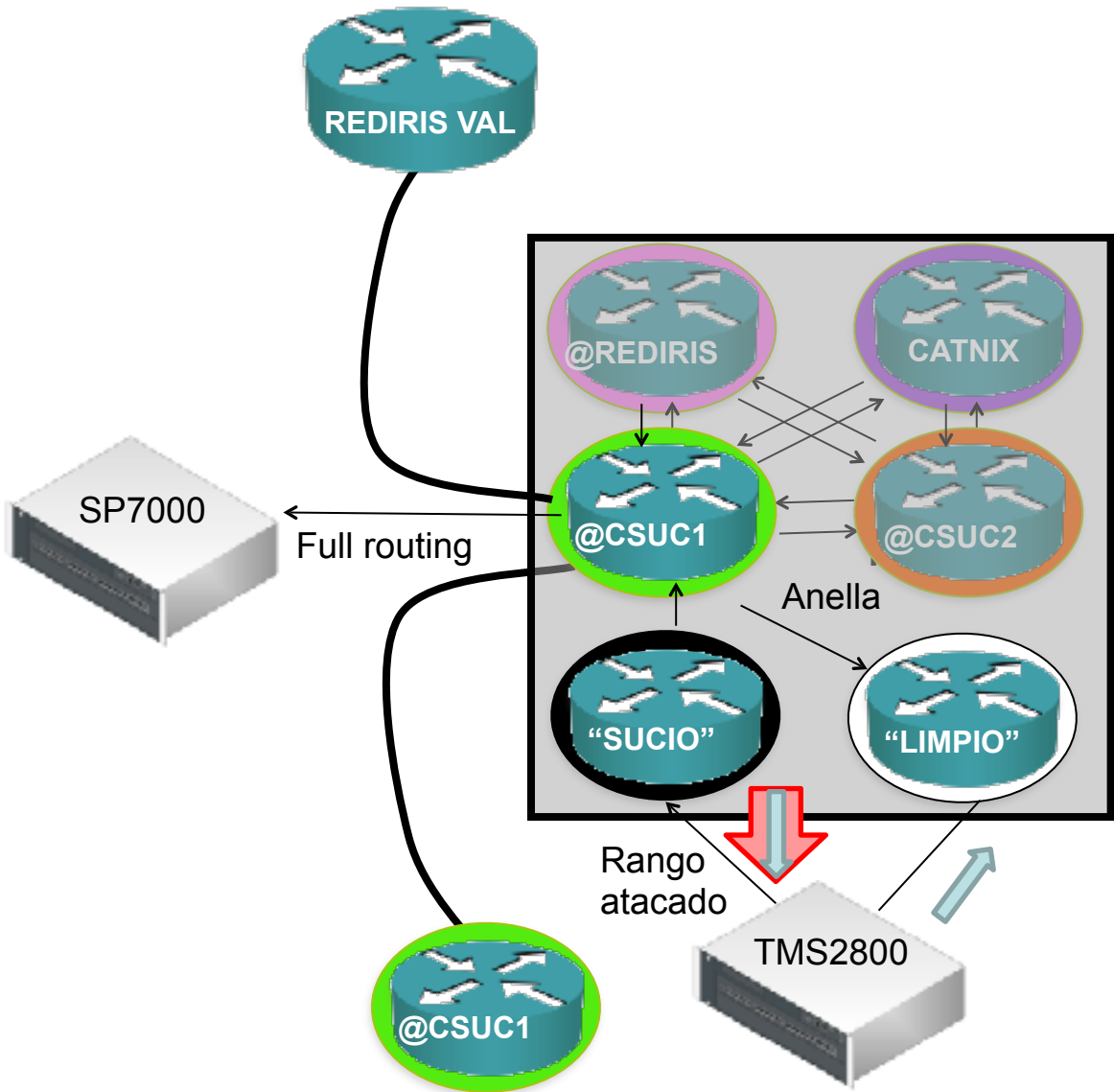
En caso de mitigación



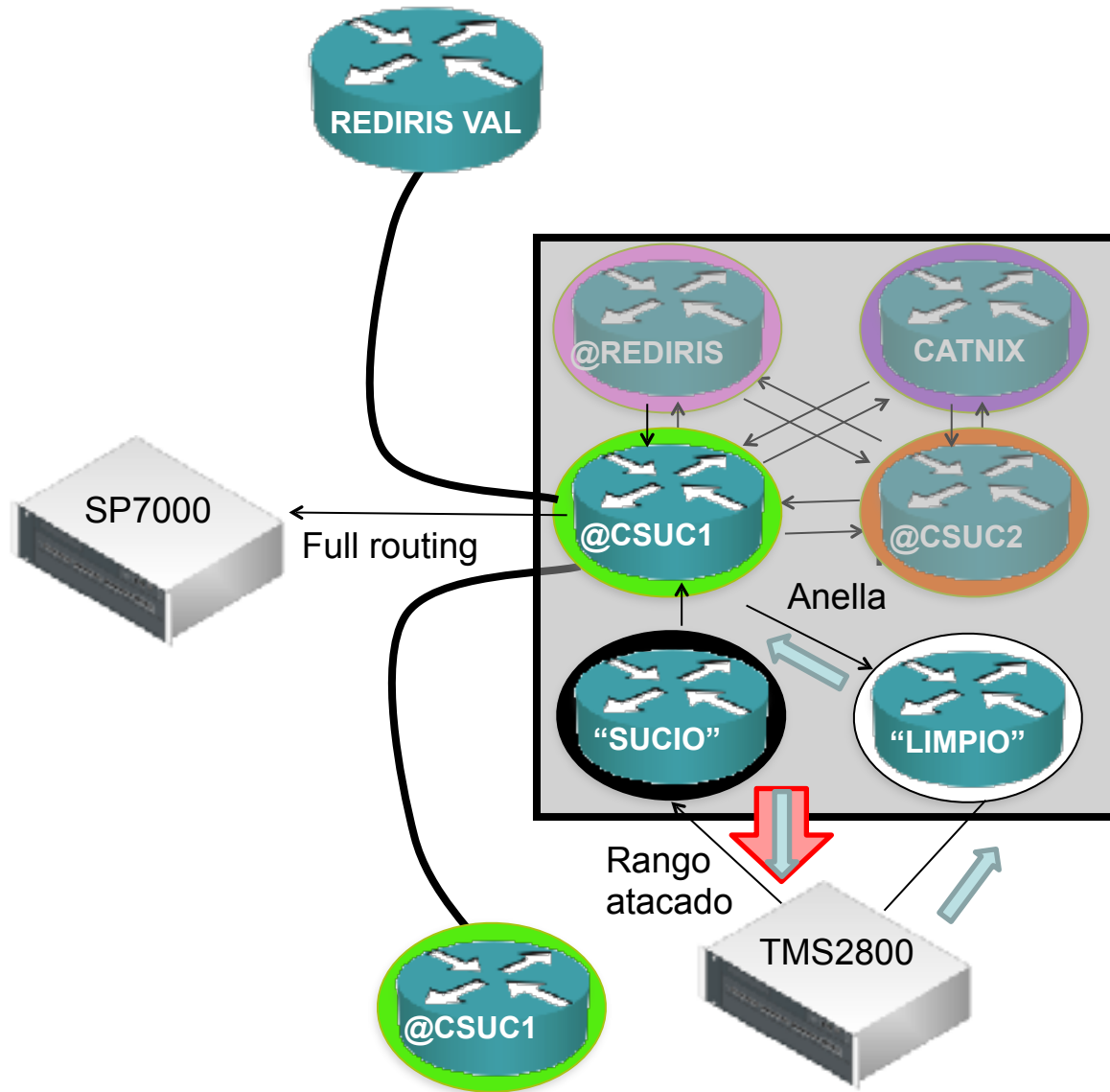
En caso de mitigación



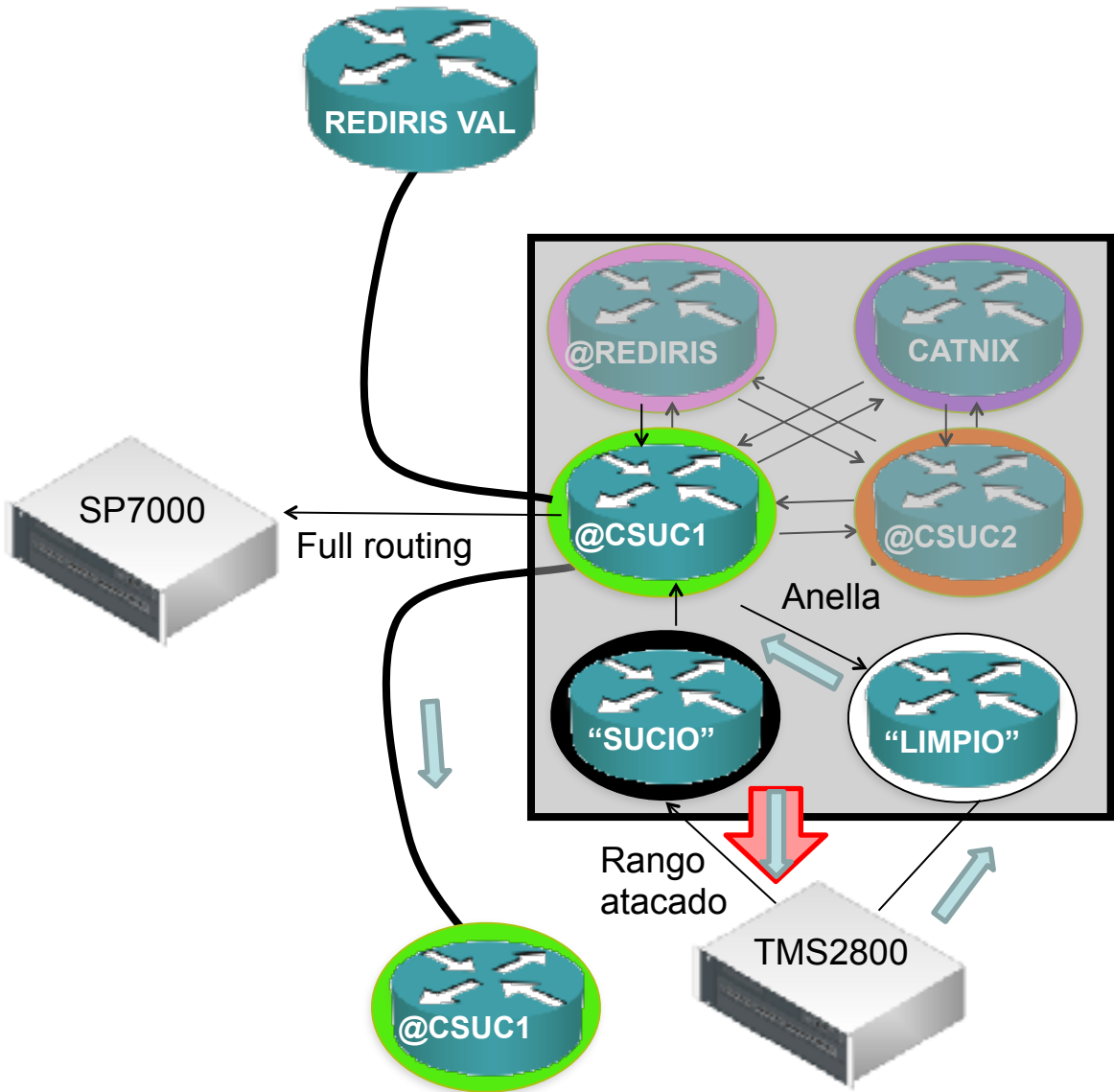
En caso de mitigación



En caso de mitigación

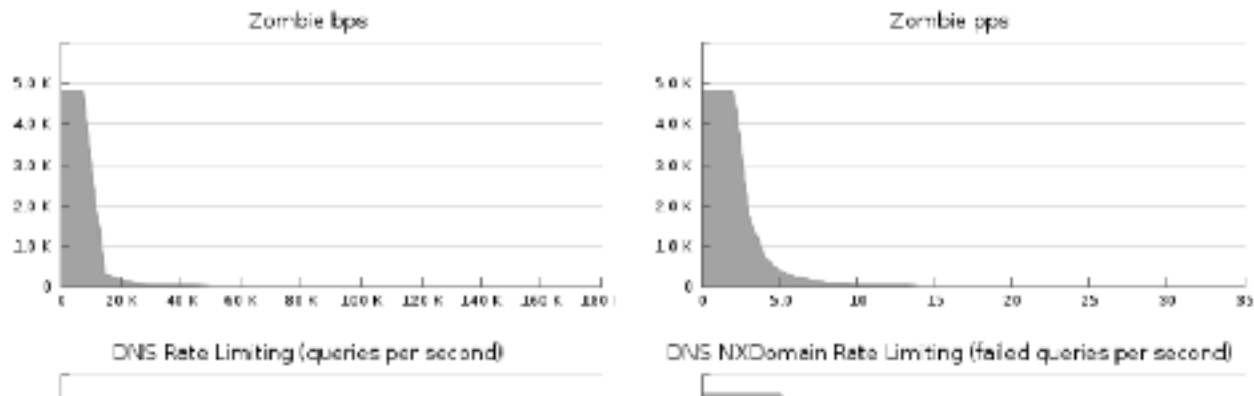


En caso de mitigación



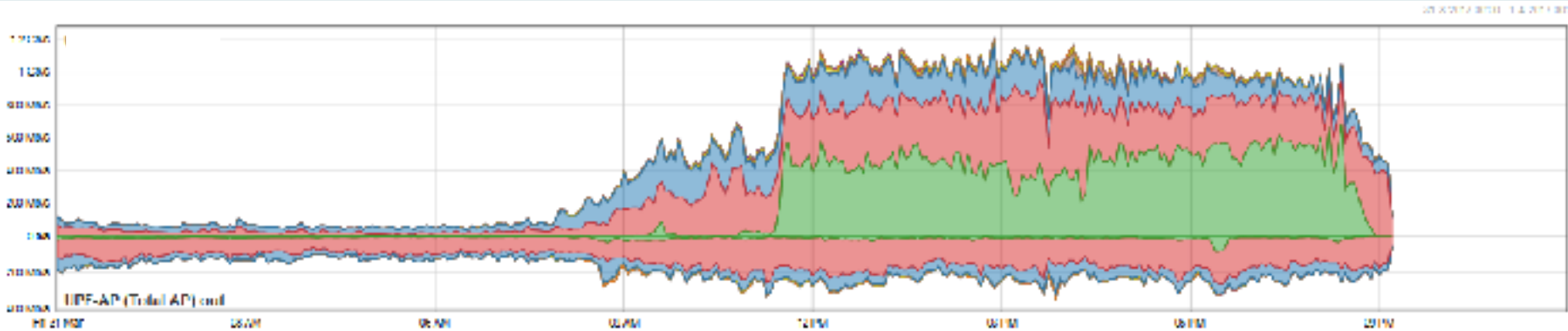
- ✓ Reuniones bilaterales con cada universidad para definir:
 - Objetos (conjunto de direcciones) a proteger.
 - Responsable(s) de autorizar mitigación para cada objeto.
 - Umbrales de detección, para evitar falsos positivos en 24x7 sin dejar de detectar ataques que afectarían a la infraestructura.
 - Parámetros de mitigación “estándar” para cada objeto.
 - Formato de los informes
- ✓ Aprendizaje para cada objeto en hora punta: base en caso de mitigación

These graphs show the number of hosts using various bandwidth levels per countermeasure.
This data was collected outside of a mitigation to be used as a baseline.

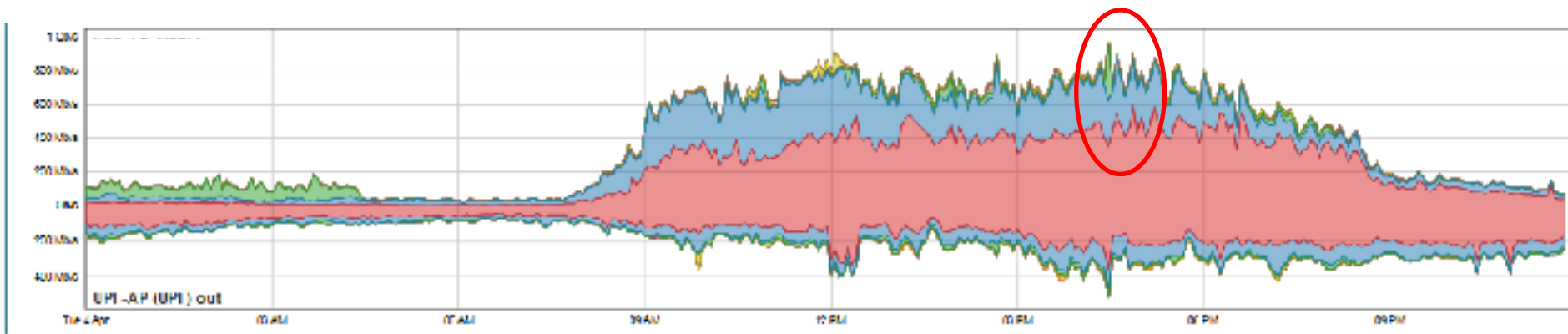


¿Qué hemos visto desde la puesta en marcha de la plataforma (1-3-2017)?

✓ No se detectó, había elecciones con e-voto... pero era tráfico legítimo



✓ Se detectó, era un ataque, avisamos... sin afectación para la universidad



¿Cómo se mitiga? Tuneando...

Managed Object: [Cisco 7700 Series Performance](#)

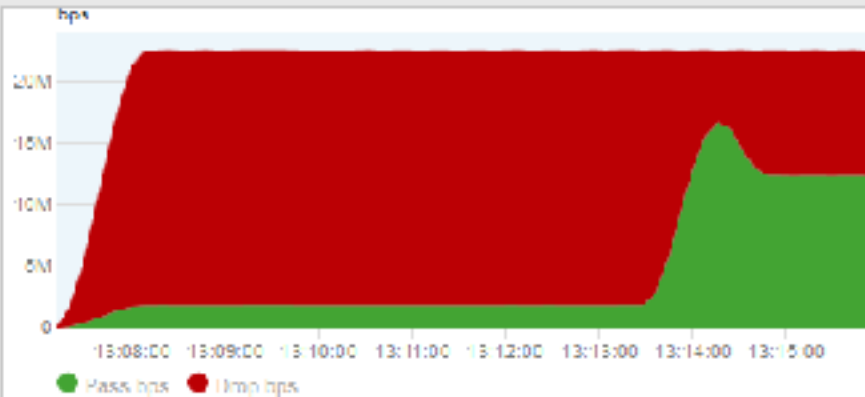
Learning Dataset

TMS Group

Diversion Prefixes

Stop

Total Per TMS Per Controller/Interface Lps Kps



Summary 30 Minutes 5 Minutes

	1 Min Avg	5 Min Avg	Summary Avg
Dropped:	10.2 Mbps	15.7 Mbps	10.7 Mbps
Passed:	12.3 Mbps	6.8 Mbps	4.5 Mbps
Total:	22.5 Mbps	22.5 Mbps	21.2 Mbps
Percent Dropped:	45.27%	69.81%	70.27%
Blocked Hosts:	0 hosts	0 hosts	0 hosts

Download Blocked Hosts

Download Top Blocked Hosts

- ON Invalid Packets
- OFF IPv4 Address Filter Lists
- ON IPv4 Black/White Lists 15.7 Mbps 4.1 Kpps
- OFF Packet Header Filtering
- OFF IP Location Filter Lists
- OFF Zombie Detection
- ON Per-Connection Load Protection
- OFF TCP SYN Authentication
- OFF DNS Scoping
- OFF DNS Authentication
- ON TCP Connection Limiting
- OFF TCP Connection Reset
- OFF Payload Regular Expression
- OFF Source /24 Rate Limit
- OFF Protocol Baselines
- OFF DNS Malformed
- OFF DNS Rate Limiting
- ON DNS NXDomain Rate Limiting
- OFF DNS Regular Expression
- OFF HTTP Malformed
- OFF HTTP Scoping
- ON HTTP Rate Limiting
- OFF ACP and HTTP/URL Regular Expression
- OFF SSL Negotiation
- ON SIP Malformed
- OFF SIP Request Limiting
- OFF Shaping
- OFF IP Location Policing

Match

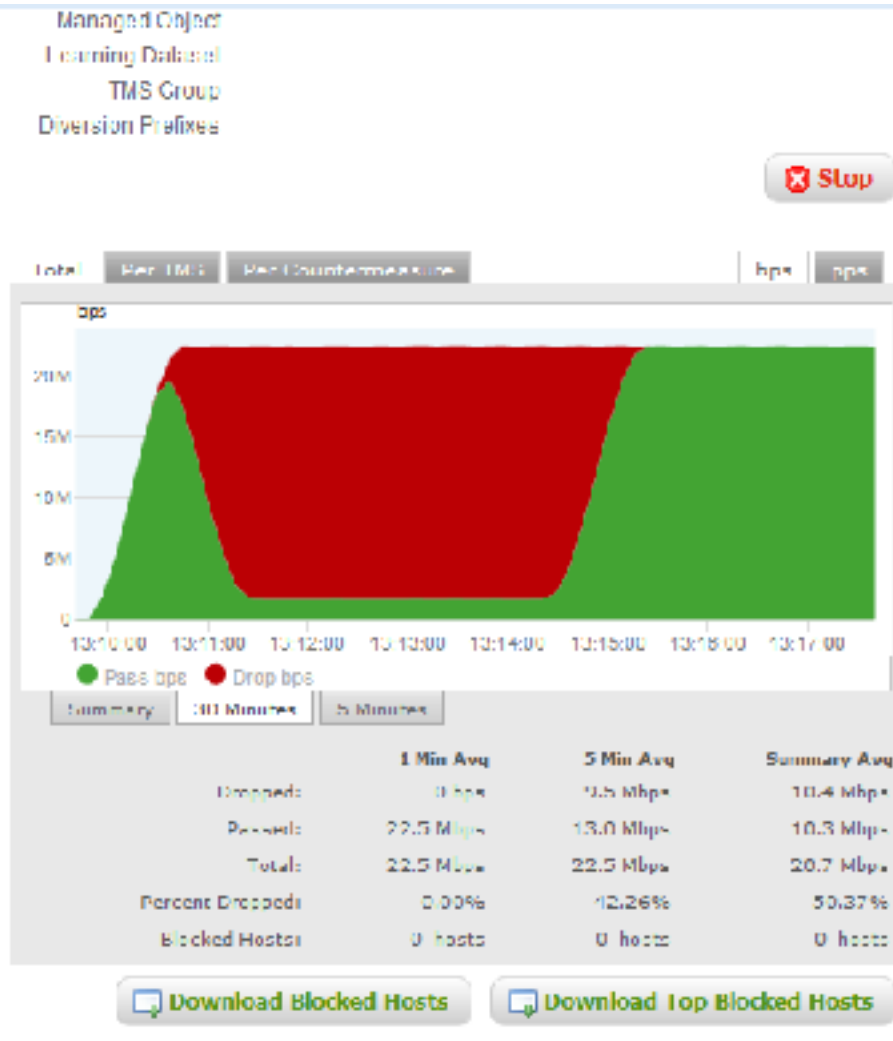
Match Type New Filter

Engageable

480 ports: 87 and proto: udp

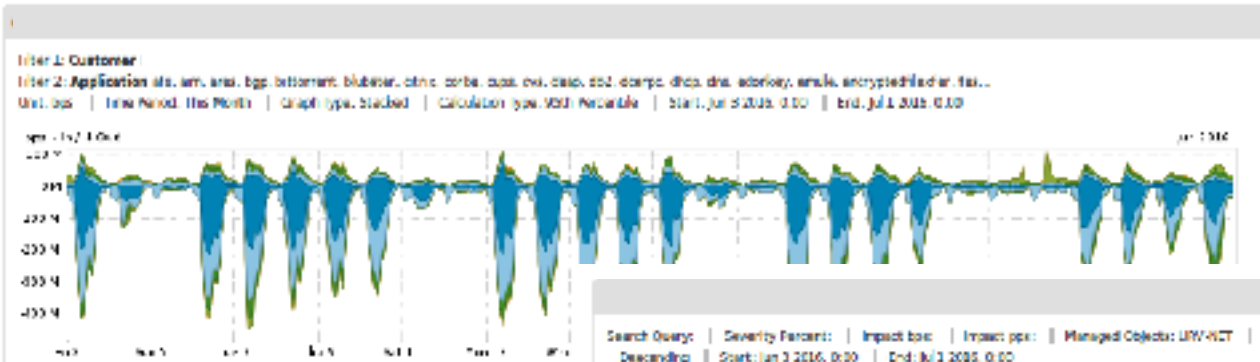
Open ECAR Wizard

¿Cómo se mitiga? Tuneando...



<input type="checkbox"/>	ON	Invalid Packets		
<input type="checkbox"/>	UI I	IPv4 Address Filter Lists		
<input type="checkbox"/>	UI I	IPv4 Block/White Lists	0.5 Mbps	2.5 Kpps
<input type="checkbox"/>	OFF	Packet Header Filtering		
<input type="checkbox"/>	OFF	IP Location Filter Lists		
<input type="checkbox"/>	OFF	Zombie Detection		
<input type="checkbox"/>	OFF	Per Connection Flood Protection		
<input type="checkbox"/>	OFF	TCP SYN Authentication		
<input type="checkbox"/>	OFF	DNS Scoping		
<input type="checkbox"/>	OFF	DNS Authentication		
<input type="checkbox"/>	UI I	TCP Connection Limiting		
<input type="checkbox"/>	UI I	TCP Connection Reset		
<input type="checkbox"/>	OFF	Payload Regular Expression		
<input type="checkbox"/>	OFF	Source /24 Baselines		
<input type="checkbox"/>	OFF	Protocol Baselines		
<input type="checkbox"/>	OFF	DNS Malformed		
<input type="checkbox"/>	OFF	DNS Rate Limiting		
<input type="checkbox"/>	OFF	DNS NXDomain Rate Limiting		
<input type="checkbox"/>	OFF	DNS Regular Expression		
<input type="checkbox"/>	UI I	UI IP Malformed		
<input type="checkbox"/>	UI I	UI IP Scoping		
<input type="checkbox"/>	OFF	HTTP Rate Limiting		
<input type="checkbox"/>	OFF	AJP and HTTP/URL Regular Expression		
<input type="checkbox"/>	OFF	SSL Negotiation		
<input type="checkbox"/>	OFF	SIP Malformed		
<input type="checkbox"/>	OFF	SIP Request Limiting		
<input type="checkbox"/>	OFF	Shaping		
<input type="checkbox"/>	OFF	IP Location Policing		

Generación de informes

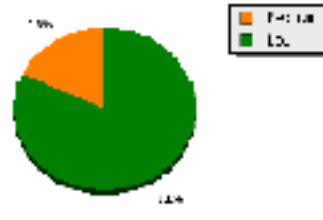


CUSTOMER	APPLICATION
10T	tel
10T	http
10T	whm-isp
10T	whm-tcp
10T	exchange-ty
10T	bitstream
10T	ssh
10T	smtp
10T	dn
10T	rt
10T	mysql
10T	gcp
10T	irc
10T	globe
10T	ppp
10T	snmp
10T	car
10T	bitnet
10T	isp
10T	corpus

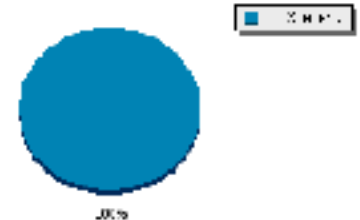


Search Query: | Severity Percent: | Impact bit: | Impact pps: | Managed Objects: UN-RGT | Limit: 1000 | Time Period: This Month | Sort Column: Alert ID | Sort Order: Descending | Start: Jun 2 2016, 0:00 | End: Jul 1 2016, 0:00

Alerts By Severity Level



Alerts By Type



ID	Graph	Importance	Alert	Start Time	Last Activation
1604		Low 55.8% of 41.4 Mbps 10.4 Mbps, 74.3 Ppps	DoS Alert Incoming P-P DoS Profile Detector: 10T-10T	Jun 24 09:15 - 09:50 (35)	Possible Attack The alert was generated because the incoming expected rates have been exceeded (baseline: 27.54 Mbps, observed: 29.67 Mbps, baseline: 2.02 Ppps, observed: 0.26 Ppps) (y-axis unnormalised)
2602		Medium 208.2% of 45.2 Mbps 11.4 Mbps, 45.2 Ppps	DoS Alert Incoming P-P DoS Profile Detector: ServiceB-Maps	Jun 28 09:15 - 10:15 (26)	Possible Attack The alert was generated because the incoming expected rates have been exceeded (baseline: 1.68 Mbps, observed: 92.0 Mbps, baseline: 1.57 Ppps, observed: 3.71 Ppps) (y-axis unnormalised)
1605		Medium 37.0% of 48.7 Mbps 12.2 Mbps, 44.3 Ppps	DoS Alert Incoming P-P DoS Profile Detector: ServiceB-Maps	Jun 28 09:15 - 10:15 (26)	Possible Attack The alert was generated because the incoming expected rates have been exceeded (baseline: 1.12 Mbps, observed: 125.0 Mbps, baseline: 0.44 Ppps, observed: 4.18 Ppps) (y-axis unnormalised)
609		Low 9.3% of 48.2 Mbps 29.5 Mbps, 29.7 Ppps	DoS Alert Incoming P-P DoS Profile Detector: 10T-10T	Jun 28 09:15 - 10:15 (26)	Possible Attack The alert was generated because the incoming expected rates have been exceeded (baseline: 1.12 Mbps, observed: 145.67 Mbps, baseline: 0.44 Ppps, observed: 4.18 Ppps) (y-axis unnormalised)

La mitigación de DDoS no es un cuento de hadas

- ✓ Parametrizar los parámetros de detección y mitigación y poner en marcha los aprendizajes en “tiempo de paz”.
- ✓ Poner en marcha una mitigación sólo en caso de emergencia.
- ✓ Es un proceso muy manual y con mucha granularidad.
- ✓ Cualquier mitigación tiene efectos colaterales indeseados.
- ✓ Es imprescindible la comunicación con la institución afectada durante la mitigación.
- ✓ No se puede dejar activa más tiempo del imprescindible.



¿Qué hacen otras redes académicas en Europa?

- ✓ Se utilizan soluciones fuera de línea, la mayoría comerciales.
- ✓ Entrenamiento para hacer *baselining*, aunque no es perfecto.
- ✓ Se usa detección automática y/o manual.
- ✓ Imprescindible consentimiento del contacto autorizado.
- ✓ Nunca mitigación no autorizada, aunque se detecte el ataque.
- ✓ Nunca mitigación automática.
- ✓ Uso de (ACL) o límites de ancho de banda (rate-limiting) en los routers.
- ✓ Filtrado de tráfico en routers antes de pasarlo a mitigación (UDP, ...).
- ✓ Si no hay más remedio -> *blackhole* (RTBH o manual)
- ✓ Para volúmenes grandes, el *upstream* debe ayudar a cortar el tráfico.
- ✓ Si se satura el *upstream*, no hay nada que hacer.
- ✓ Poco extendidas las soluciones comerciales en Cloud.
- ✓ Poco extendido el uso de FlowSpec.
- ✓ Iniciativas conjuntas a nivel de Géant. (FoD, DDoS workshop)

Cuando no queda más remedio...blackholing

- ✓ Es una medida de contingencia para parar los DDoS volumétricos.
- ✓ Implica mandar el tráfico de una cierta IP a Null0.
- ✓ Como el ataque proviene de miles de direcciones cambiantes, se le hace blackholing al atacado (el tráfico de la propia entidad).
- ✓ Se deniega el tráfico legítimo.
- ✓ Al denegar la IP atacada se descongestiona la línea y el resto de direcciones siguen funcionando.
- ✓ En ocasiones se abusa del blackholing denegando direcciones no atacadas (por ejemplo, IP de la competencia).



Colaboración con RedIRIS: detección CSUC, mitigación vía túnel RedIRIS

- ✓ Solución de mitigación de RedIRIS
- ✓ Detección: institución o CSUC
- ✓ Mitigación: 2 túneles (direccionamiento RedIRIS/CSUC):
 - Requiere el visto bueno de la institución.
 - Configuración manual por parte de RedIRIS.
 - Hasta 1,5 Gbps.
 - Probada con direcciones “señuelo” de las universidades.
 - RedIRIS anuncia el rango atacado y lo desvía a su equipo de mitigación
 - El tráfico hacia las IP atacadas se limpia y se entrega por los túneles
- ✓ Estos túneles se mantienen como solución “aguas arriba” en caso necesario

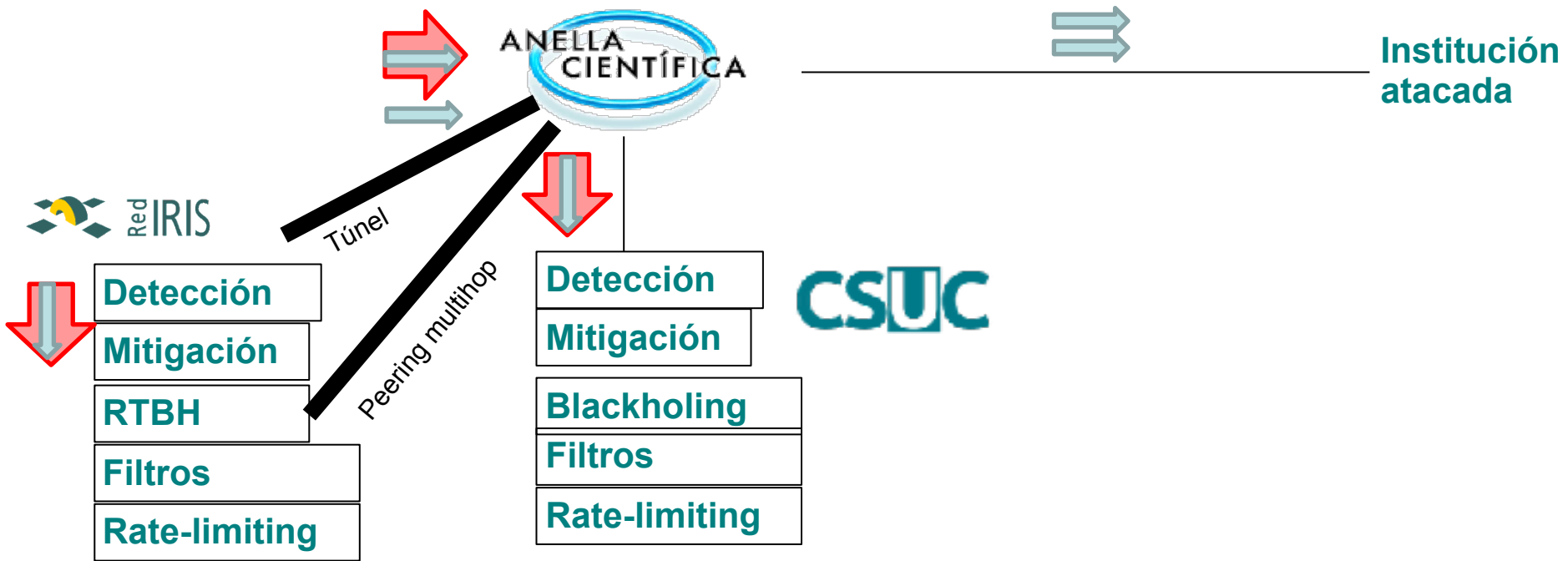


Más colaboración con RedIRIS: Remote Triggered Blackholing (RTBH)

- ✓ El filtrado RTBH es una técnica que usa updates de BGP para manipular las tablas de routing en otros puntos de la red antes de entrar en la red atacada.
- ✓ El equipo que lanza el trigger provoca que los routers lancen el tráfico a Null0 (blackhole).
- ✓ Es una forma rápida de solicitar el filtrado y de quitarlo por parte del proveedor atacado.
- ✓ En marcha sesión BGP con RedIRIS para el blackholing de las direcciones del AS de la Anella Científica



Cuantos más mecanismos, más opciones en caso de ataque



- ✓ Flowspec permite especificar información del flujo y aplicar filtros automáticamente en los routers.
- ✓ El objetivo es interactuar con la red para modificar su comportamiento.
- ✓ Es una forma de aprovisionar ACL y PBR vía MP-BGP.
- ✓ Permite:
 - ✓ Hacer drop
 - ✓ Aplicar QoS
 - ✓ Rate-limit (0 sería un blackhole)
 - ✓ Marcar el tráfico
 - ✓ Redirigir el tráfico
 - ✓ ...
- ✓ Los equipos que se instalarán este semestre en el troncal soportan Flowspec.

- ✓ Aplicar siempre filtros anti-spoofing.
- ✓ Limpiar infecciones.
- ✓ Tener logs con la hora sincronizada vía NTP.
- ✓ Identificar a los usuarios (cuidado con el NAT!).
- ✓ En caso de ataque, reportar a la policía.
- ✓ Tener en cuenta que dependiendo del ataque:
 - Puede ser grave y que sólo lo detecta el atacado.
 - Puede ser inofensivo y ser detectado en monitorización.
- ✓ Ser conscientes de que no hay una solución que lo mitigue todo, la mitigación es en capas (NREN, RREN, firewall institución,...).



Consorti de
Serveis Universitaris
de Catalunya

¡Gracias por vuestra atención!

¿Preguntas?

mariaisabel.gandia@csuc.cat

