Alai Secure

Soluciones profesionales para empresas de Seguridad

Riesgos y aporte de valor en los sistemas de seguridad IP

Nuevas propuestas en Seguridad Telco

Eduardo Mohedano
Executive Infrastructure Architect
ALAI Telecom

Evolución de los sistemas de vigilancia y alarma por datos móviles

Alai Secure

www.alaisecure.com

Situación inicial de la seguridad basada en GPRS

Las **tarjetas SIM** fueron una revolución en el sector Seguridad:

1) Sin cable (ADSL/FTTH).

2) Mejor precio – independencia.

3) Bidireccionalidad.

4) Funcionaban con APN's públicos del operador.

5) Rápidamente se pusieron de manifiesto sus riesgos:
   - Sistemas en Internet abierto.
   - Visibles para los clientes y para el resto del mundo también.
   - Vulnerables a barridos de datos, hackeos, ataques DoS, fraude, etc...

Evolución de las comunicaciones GPRS
(El paso de la securización "APN privado + VPN")

1) Algunos operadores de telecomunicaciones comenzaron a ofrecer seguridad ante las reclamaciones: 1) **APN privado** **2) VPN**

   •Este procedimiento permite acceder a los dispositivos de forma segura (añadieron una capa de seguridad importante y necesaria).

2) Funcionar con VPN del operador implica:
   - •Sistemas no visibles en Internet.
   - •Posibilidad de salida a Internet si lo necesitan.
   - •No son susceptibles a barridos de datos, ataques DoS, hackeos, fraude...

Con este sistema conseguimos un paso importante....

Situación actual comunicaciones GPRS
(La evolución del mercado: La nube de los fabricantes)

- Hay una tendencia creciente en el mercado.... VER EN TIEMPO REAL LAS CÁMARAS DE UN NEGOCIO, DEL HOGAR, etc...
- Para ello cada vez más, se accede a través del CLOUD del fabricante.
- Se promueve la necesidad en el usuario: Si no ofreces esto, te quedas fuera.

La idea es muy atractiva pero...
¿Qué implica esto en las comunicaciones?

Situación actual comunicaciones GPRS
(La evolución del mercado: La nube de los fabricantes)

Aumentar la inseguridad y el riesgo:

- Funcionar con APN públicos del operador para tener salida a Internet.
- Pueden llegar a ser visibles para el resto del mundo también.
- Más vulnerabilidades: barridos, ataques DDoS, hackeos, fraude...

VOLVEMOS ATRÁS... ES UNA INVOLUCIÓN

Los nuevos riesgos del IoT y el M2M

Alai Secure

www.alaisecure.com

Dispositivos IoT/M2M abiertos a Internet

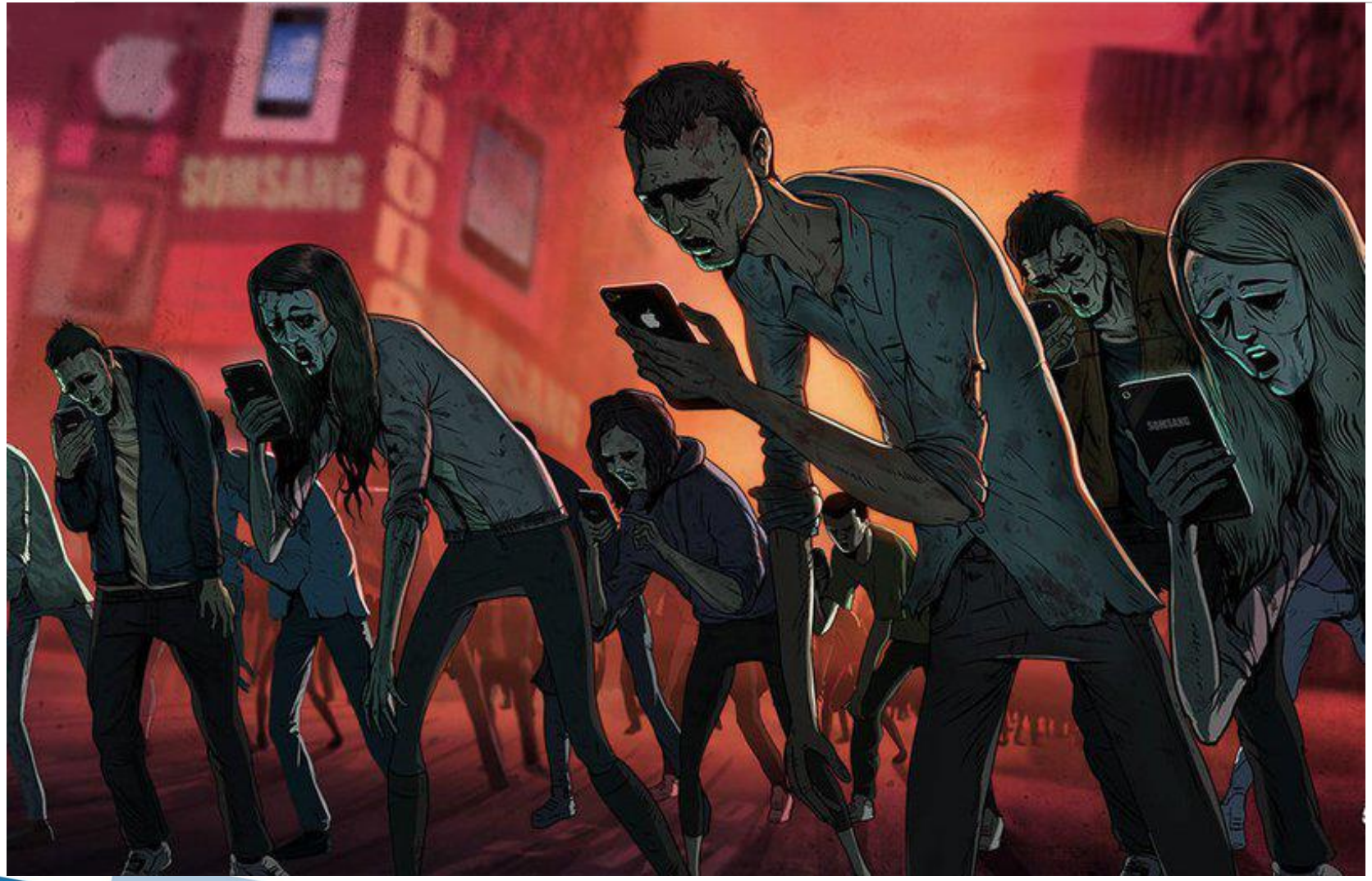
Agujeros de seguridad en 189 gasolineras de toda España

La Voz de Galicia

«Hackers» éticos de Vigo alertan a la UE de fallos de seguridad en gasolineras

Entre cinco y siete estaciones de servicio en riesgo están ubicadas en Galicia

Botnets (las redes de dispositivos zombies)



MIRAI: 21-octubre-2016, el Pearl Harbor del IoT

MIRAI: La repercusión mediática

DDoS: Varios ciberataqu

tecnologia.elpais.com/tecnologia/2016/10/21/actualidad/1477059125_058324.html?rel=mas

EL PAÍS

TECNOLOGÍA

ATAQUE A TWITTER Y OTRAS COMPAÑÍAS ›

Varios ciberataques masivos inutilizan las webs de grandes compañías

Son los más graves de la última décad

220

BEATRIZ GUILLÉN | JOAN FAUS | ROSA JIMÉNEZ CAN

Madrid / Washington / San Francisco - 22 OCT 2016 - 19:01

Una oleada de ciberata
interrumpieron este vi
medios de comunicaci
o *The New York Times*

DDoS: Varios ciberataqu

tecnologia.elpais.com/tecnologia/2016/10/21/actualidad/1477059125_058324.html?rel=mas

EL PAÍS

TECNOLOGÍA

CIBERATAQUE A TWITTER Y OTRAS WEBS ›

Así han atacado los 'hackers' las webs de Twitter, Spotify o Ebay

Varios ciberataques masivos han inutilizado numerosas páginas de grandes empresas

5

BEATRIZ GUILLÉN

22 OCT 2016 - 14:33 CEST

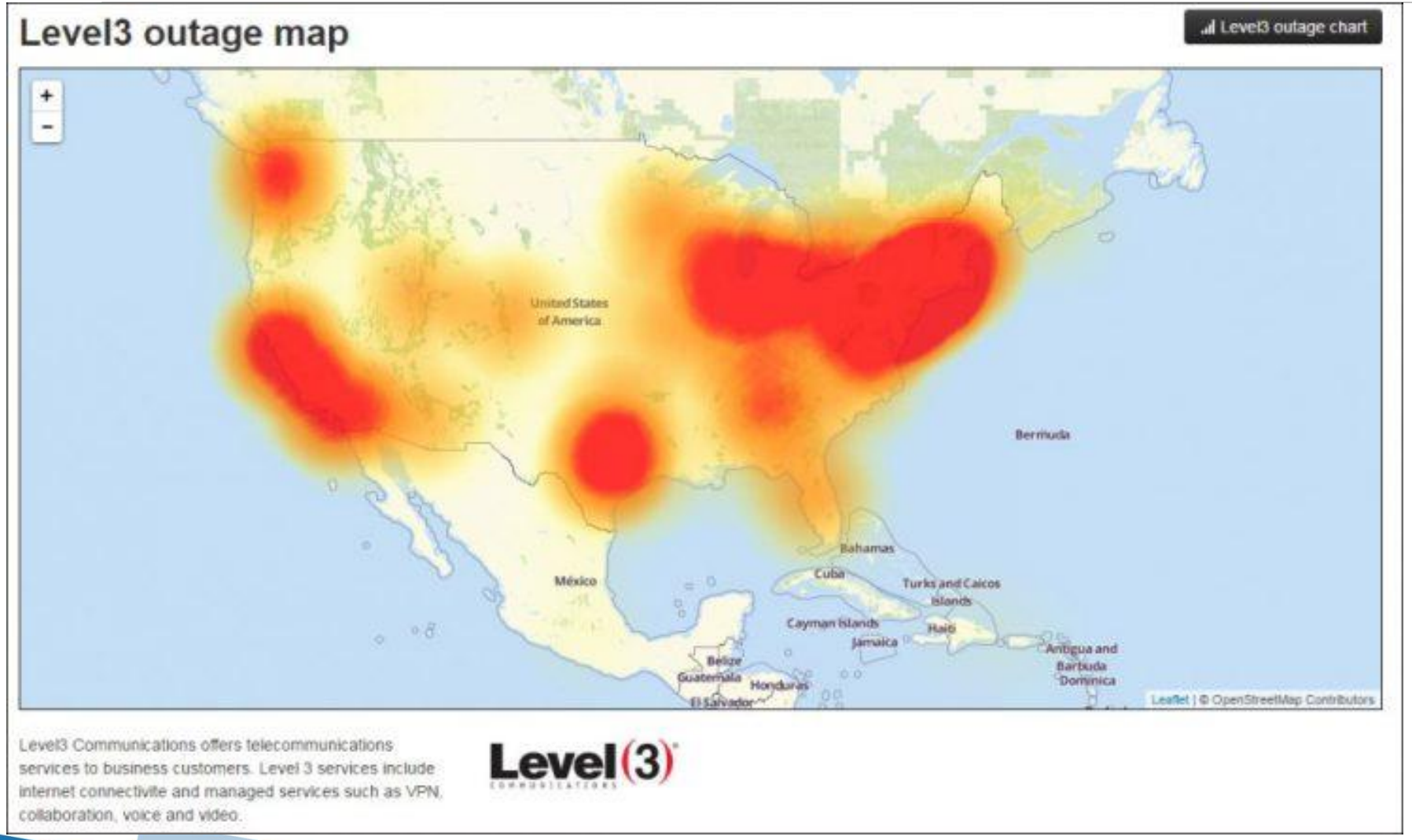
Este viernes, uno de los grandes proveedores de Internet, la empresa Dyn, ha sufrido varios ciberataques seguidos que han puesto en jaque el funcionamiento de las páginas web de muchas grandes empresas, entre las que se encuentra Twitter, Spotify, Ebay o el periódico *The New York Times*. Ha sufrido un ataque de denegación de servicio, más conocido como DDoS por sus siglas en inglés, que ha provocado problemas de conexión en todo el mundo.

"Los ataques DDoS son bastante simples de originar, pero mucho más complejos de parar", explica el director de seguridad de S2 Grupo, Antonio Villalón. El funcionamiento es sencillo: millones de dispositivos intentan acceder al mismo tiempo a una página web, de manera, que esta no puede aguantar la saturación de tráfico y se colapsa. Empieza a prestar el servicio de una manera mucho más lenta o, en el

Es como si de repente llegan a una carretera dos millones de coches. ¿Qué ocurre? Se colapsa.
"

MIRAI: los ATACADOS (Dyn en USA)

MIRAI: los ATACADOS



MIRAI: los AFECTADOS

- 2 oleadas de ataques DDoS apuntando a los servidores DNS de **Dyn** provocaron indisponibilidad a millones de usuarios en USA y Europa.
- Los principales servicios de Internet afectados fueron:

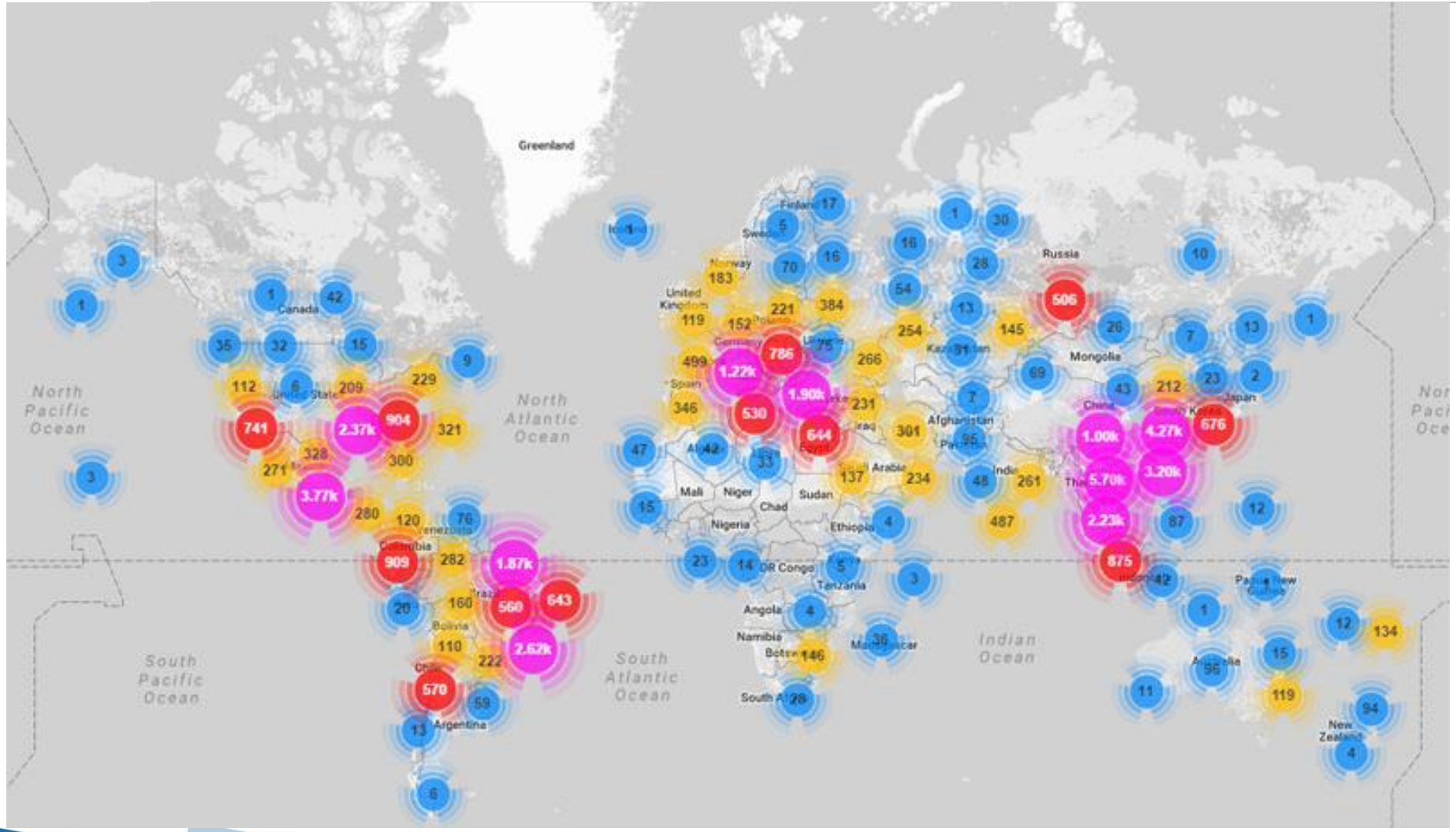
- Airbnb[11]
- Amazon.com[8]
- Ancestry.com[12][13]
- *The A.V. Club*[14]
- BBC[13]
- *The Boston Globe*[11]
- Box[15]
- *Business Insider*[13]
- CNN[13]
- Comcast[16]
- CrunchBase[13]
- DirecTV[13]
- *The Elder Scrolls Online*[13][17]
- Electronic Arts[16]
- Etsy[11][18]
- FiveThirtyEight[13]
- Fox News[19]
- *The Guardian*[19]
- GitHub[11][16]
- Grubhub[20]
- HBO[13]
- Heroku[21]
- HostGator[13]
- iHeartRadio[12][22]
- Imgur[23]
- Indiegogo[12]
- Mashable[24]
- National Hockey League[13]
- Netflix[13][19]
- *The New York Times*[11][16]
- Overstock.com[13]
- PayPal[18]
- Pinterest[16][18]
- Pixlr[13]
- PlayStation Network[16]
- Qualtrics[12]
- Quora[13]
- Reddit[12][16][18]
- Roblox[25]
- Ruby Lane[13]
- *RuneScape*[12]
- SaneBox[21]
- Seamless[23]
- *Second Life*[26]
- Shopify[11]
- Slack[23]
- SoundCloud[11][18]
- Squarespace[13]
- Spotify[12][16][18]
- Starbucks[12][22]
- Storify[15]
- Swedish Civil Contingencies Agency[27]
- Swedish Government[27]
- Tumblr[12][16]
- Twilio[12][13]
- Twitter[11][12][16][18]
- Verizon Communications[16]
- Visa[28]
- Vox Media[29]
- Walgreens[13]
- *The Wall Street Journal*[19]
- Wikia[12]
- *Wired*[15]
- Wix.com[30]
- WWE Network[31]
- Xbox Live[32]
- Yammer[23]
- Yelp[13]
- Zillow[13]

MIRAI: los ATACANTES

MIRAI: los ATACANTES

¡Un ejército de 100.000 dispositivos IoT!

MIRAI: los ATACANTES (procedencia)



Alai Secure

MIRAI: los ATACANTES (procedencia)

•164 países infectados.
•Casi 50.000 direcciones IP diferentes.

Country	% of Mirai botnet IPs
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

MIRAI: el vector de ataque

FASES del vector de ataque típico en botnets

1) **Localización**: de dispositivos IoT vulnerables mediante escaneo masivo de direcciones IP en Internet.

2) **Infiltración**: ataque a las credenciales (fuerza bruta o simplemente contraseña por defecto).

3) **Reclutamiento**: se incluyen en el botnet.

4) **Ataque DDoS**: desde los dispositivos IoT que siguen instrucciones de un centro de control remoto (C&C).

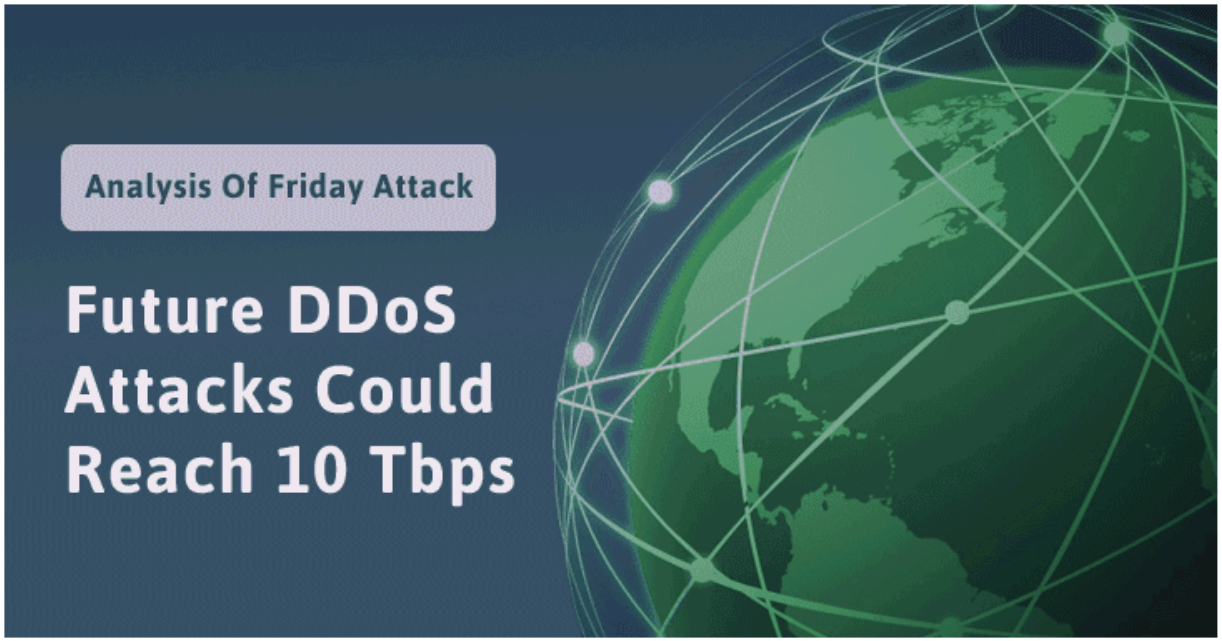
Los ataques DoS del futuro

The Hacker News™
Security in a serious way

Friday's Massive DDoS Attack Came from Just 100,000 Hacked IoT Devices

Wednesday, October 26, 2016 Swati Khandelwal

Share 13 Share Tweet Share



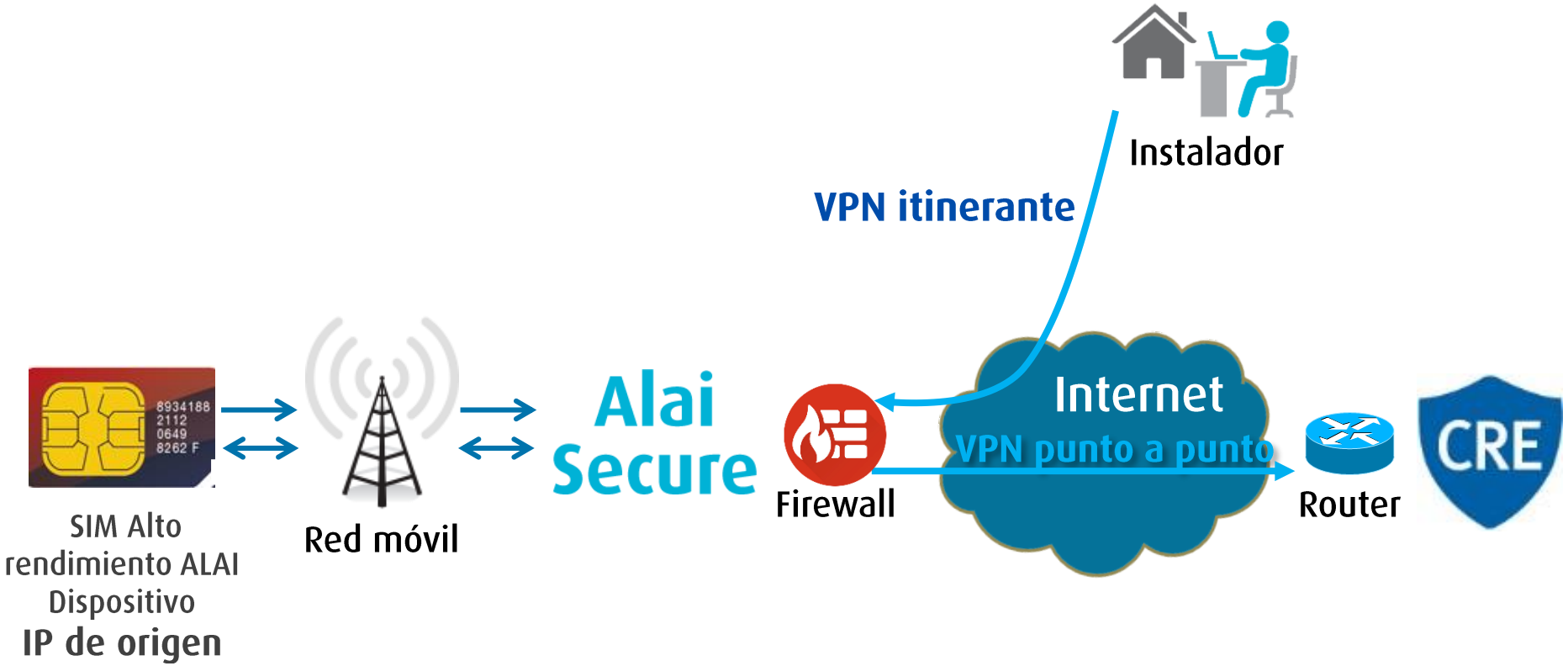
El Dilema del Riesgo

¿Ser o no ser?
¿Qué es menos malo?
¿Ser el atacante?
¿O ser el atacado?

¿Qué podemos hacer?

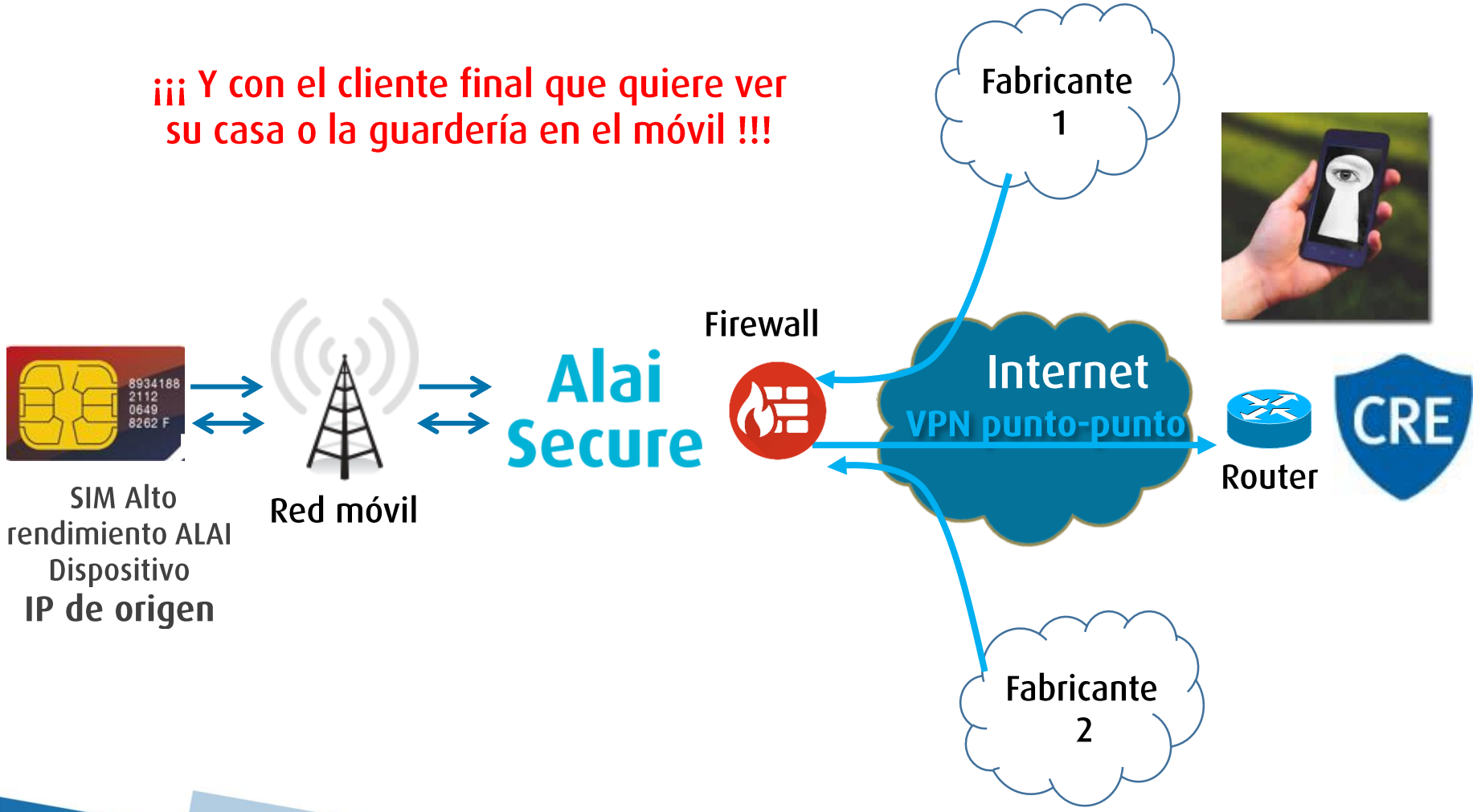
La CRE no está sola en la aventura

VPN punto a punto (CRE) + VPN Itinerante (Instalador)



Conexión con clouds de fabricantes

¡¡¡ Y con el cliente final que quiere ver su casa o la guardería en el móvil !!!



El RIESGO también está DENTRO

Para sortear los firewalls, los dispositivos inician y mantienen conexiones hacia Internet:

Actualizaciones de software
WhatsApp
Facebook
Skype
Twitter
Youtube
Y muchas más Apps...

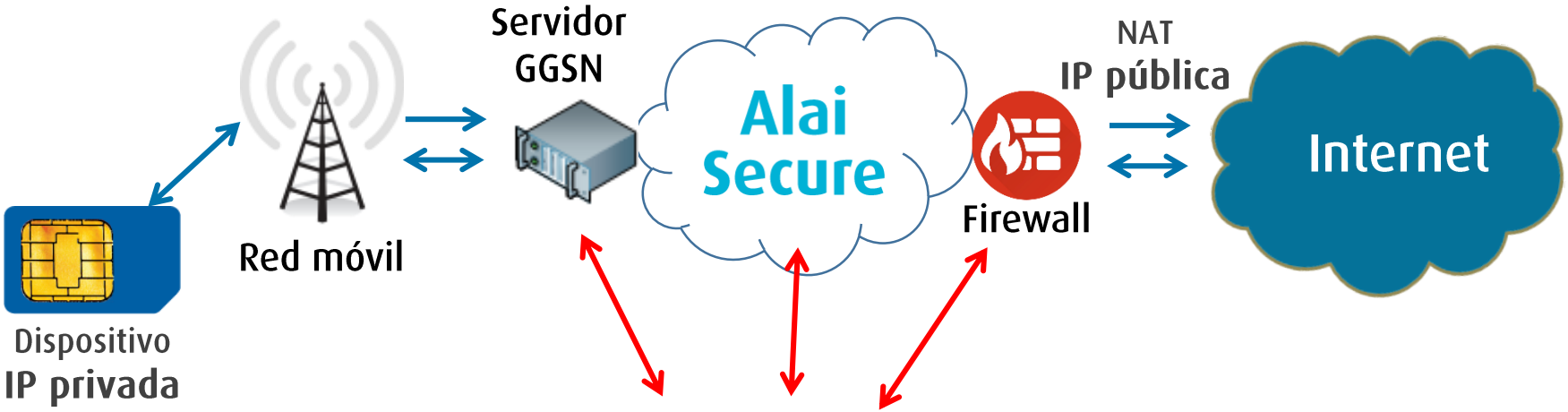
Utilizar el escenario idóneo...
(Clouds y VPN Simultáneamente)

- Utilizar un sistema de ALAI Secure con un **único APN** (olvidarse de público o privado..)
- Un sistema seguro que permite acceder bidireccionalmente a los dispositivos a través de **VPN**.
- Que además permita acceder a los **clouds de los fabricantes** ÚNICAMENTE que DECIDA la CRE, siendo personalizable.
- Un sistema con una única configuración para todo y **SIN SALIDA A INTERNET**.
- Un sistema completo, seguro y robusto, pensado y adecuado a las **necesidades de las CRE´s e instaladores**.

Una sola configuración para todo y evitando fraudes, ataques, etc...

Un servicio by Alai Secure

Arquitectura de la Red de Datos de ALAI Telecom



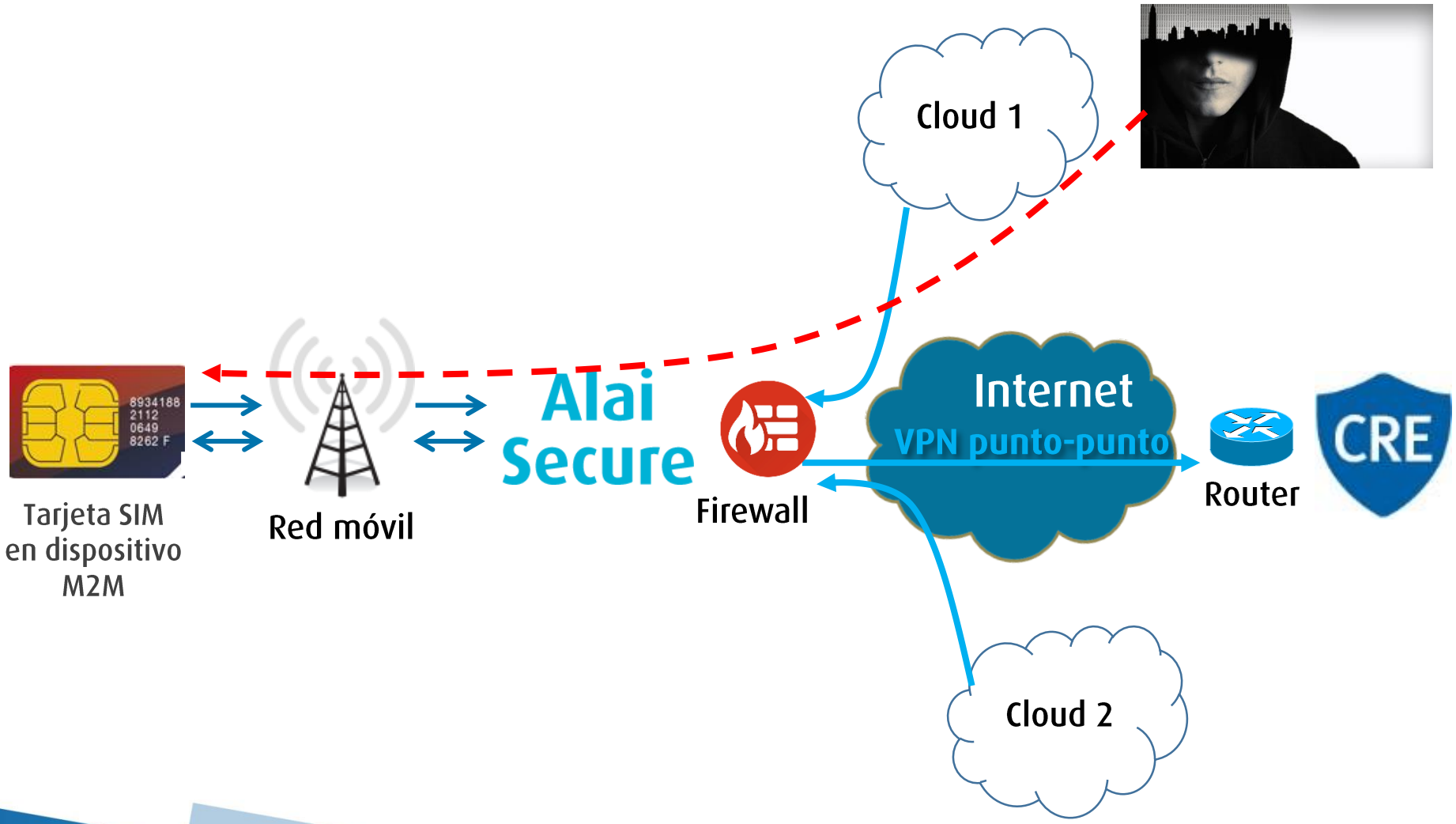
- Control
- Flexibilidad
- Gestión y monitorización.
- Escalabilidad
- Seguridad
- Personalización.
- Servicios bajo demanda

- Asignación de IPs.
- Redirección del tráfico.
- Filtrado personalizado.
- Entrega directa del tráfico.
- Integración con Radius.
- Accounting y auditoría.
- Gestión del DNS.
- Alertas de monitorización.
- Etc...

Riesgos y dilemas de los clouds

Alai Secure

Riesgo: Infiltración desde clouds



El Dilema del Negocio

¿De quién son los clientes finales?
¿De la empresa de Seguridad?
¿O de los fabricantes de equipos?

Opción: Conexión con clouds a través de la CRA

Cloud 1

8934188
2112
0649
8262 F

SIM Alto rendimiento ALAI Dispositivo

IP de origen

Red móvil

Alai Secure

Firewall

Internet

VPN punto-punto

Router

CRE

Cloud 2

La Cadena de Valor

¿Quién aporta el valor a los clientes finales?

- ¿La CRA?
- ¿El instalador?
- ¿El fabricante de los equipos?
- ¿El operador Telco?
- ¿El ISP?
- ¿El cloud? ¿La nube?
- ¿Quién está detrás de la nube?

El dilema de Hamlet

Ser o no ser, ésa es la cuestión.
¿Es de más noble espíritu
sufrir las arremetidas
y los dardos de la adversa fortuna
o, por el contrario,
empuñar las armas contra
un mar de adversidades
y terminar con ellas
haciéndoles frente?

(Hamlet, William Shakespeare)

Alai Secure

Operador global en Seguridad Telco

Muchas gracias

Eduardo Mohedano

Executive Infrastructure Architect

Eduardo.Mohedano@alai.es

Condesa de Venadito 1, 11ª plta

28027 Madrid

Tarragona, 157 4ª plta

08015 Barcelona

www.alaisecure.com