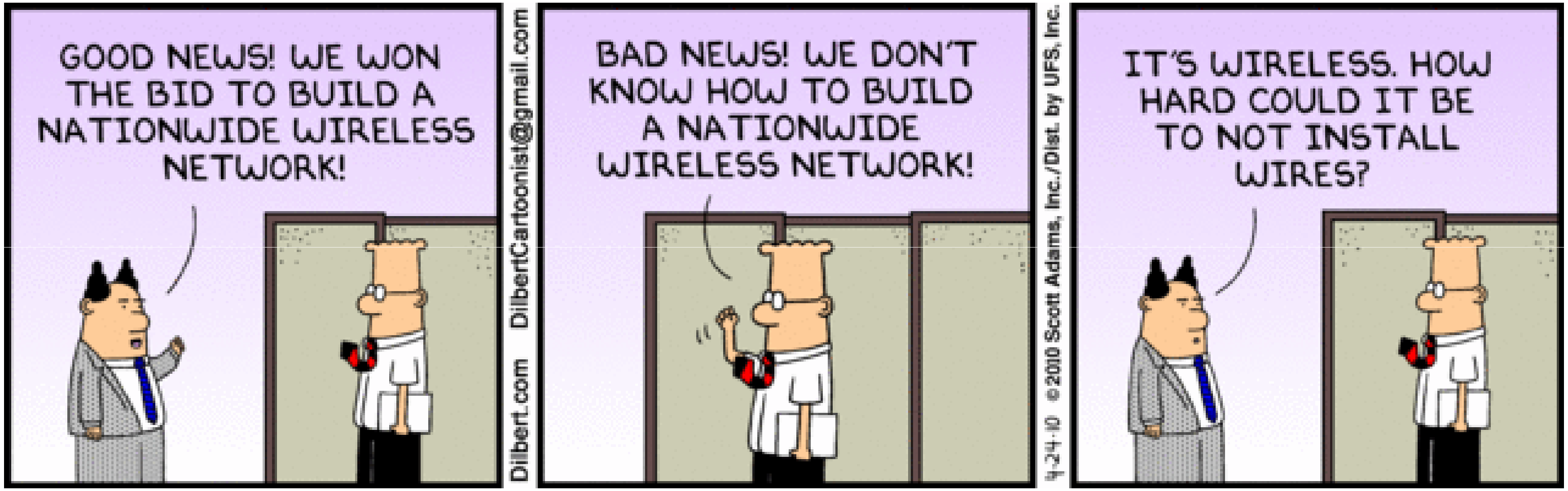
Arquitectura segura y gestión de amenazas en despliegues wifi

Toni Pérez
toni.perez (at) uib.es

Universitat de les Illes Balears
Centre de Tecnologies de la Informació

GOOD NEWS! WE WON THE BID TO BUILD A NATIONWIDE WIRELESS NETWORK!
Dilbert.com DilbertCartoonist@gmail.com
BAD NEWS! WE DON'T KNOW HOW TO BUILD A NATIONWIDE WIRELESS NETWORK!
4-24-10 © 2010 Scott Adams, Inc./Dist. by UFS, Inc.
IT'S WIRELESS. HOW HARD COULD IT BE TO NOT INSTALL WIRES?

¿Puede ser segura la wifi?

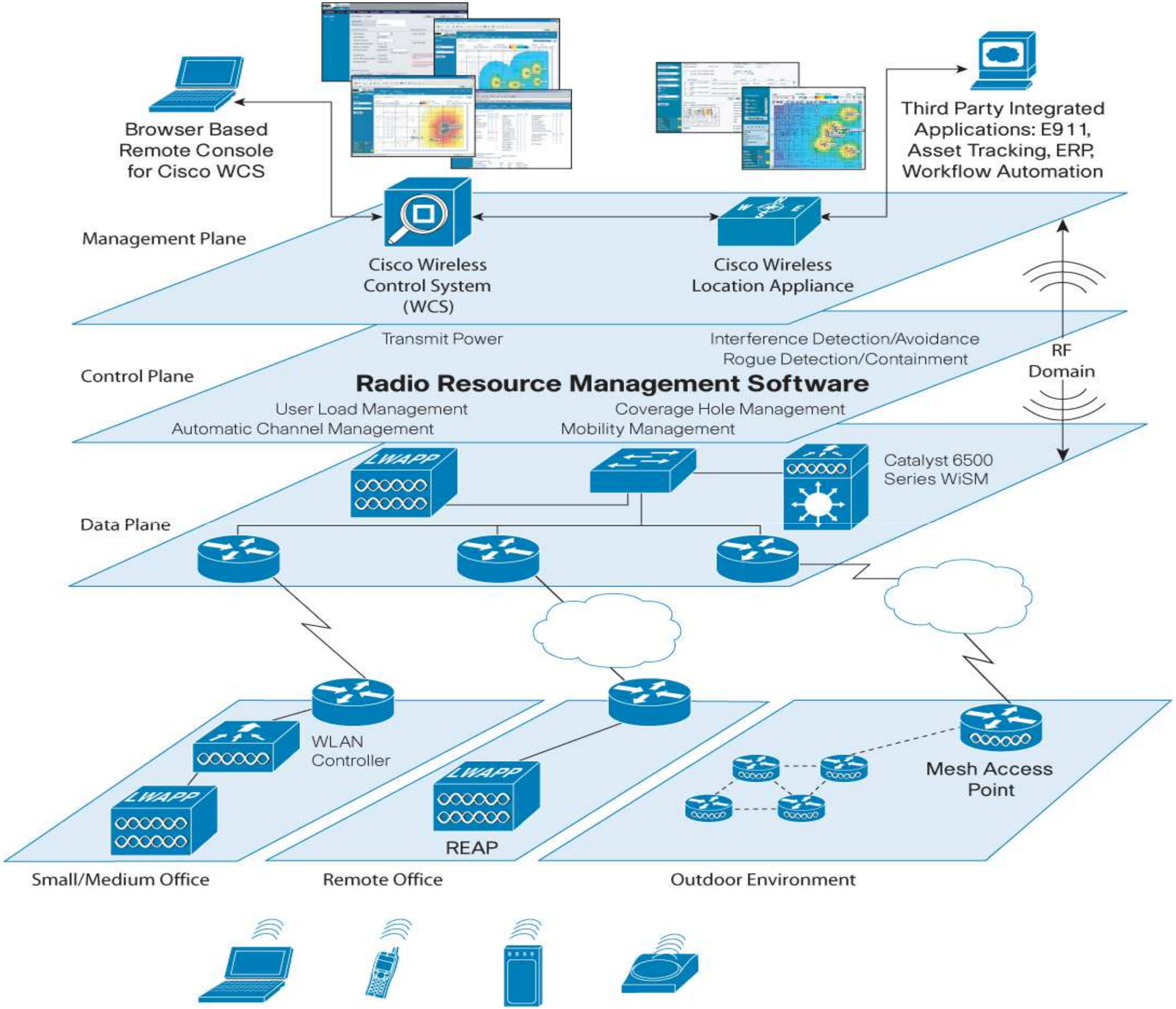
- Segura si! Alta disponibilidad…nunca!
  - Disponibilidad vulnerable a nivel 1 y 2
  - Seguridad equivalente al cableado
  - Necesario acceso 802.1x/TLS y cifrado AES
- Pero… ¿podremos ser tan estrictos?
  - Os suena:
    - "Este cacharro tiene wifi y sólo soporta wep"
    - "Estos invitados necesitan wifi inmediatamente"

¿Qué estamos securizando?

- Un servicio complementario no crítico
  - Complementa al cableado existente, no lo substituye
- Movilidad en un entorno heterogéneo
  - Simplificar el servicio
    - 802.1X es lo más cómodo... una vez configurado
  - Gran diversidad de terminales y versiones
  - Usuarios con diferentes necesidades

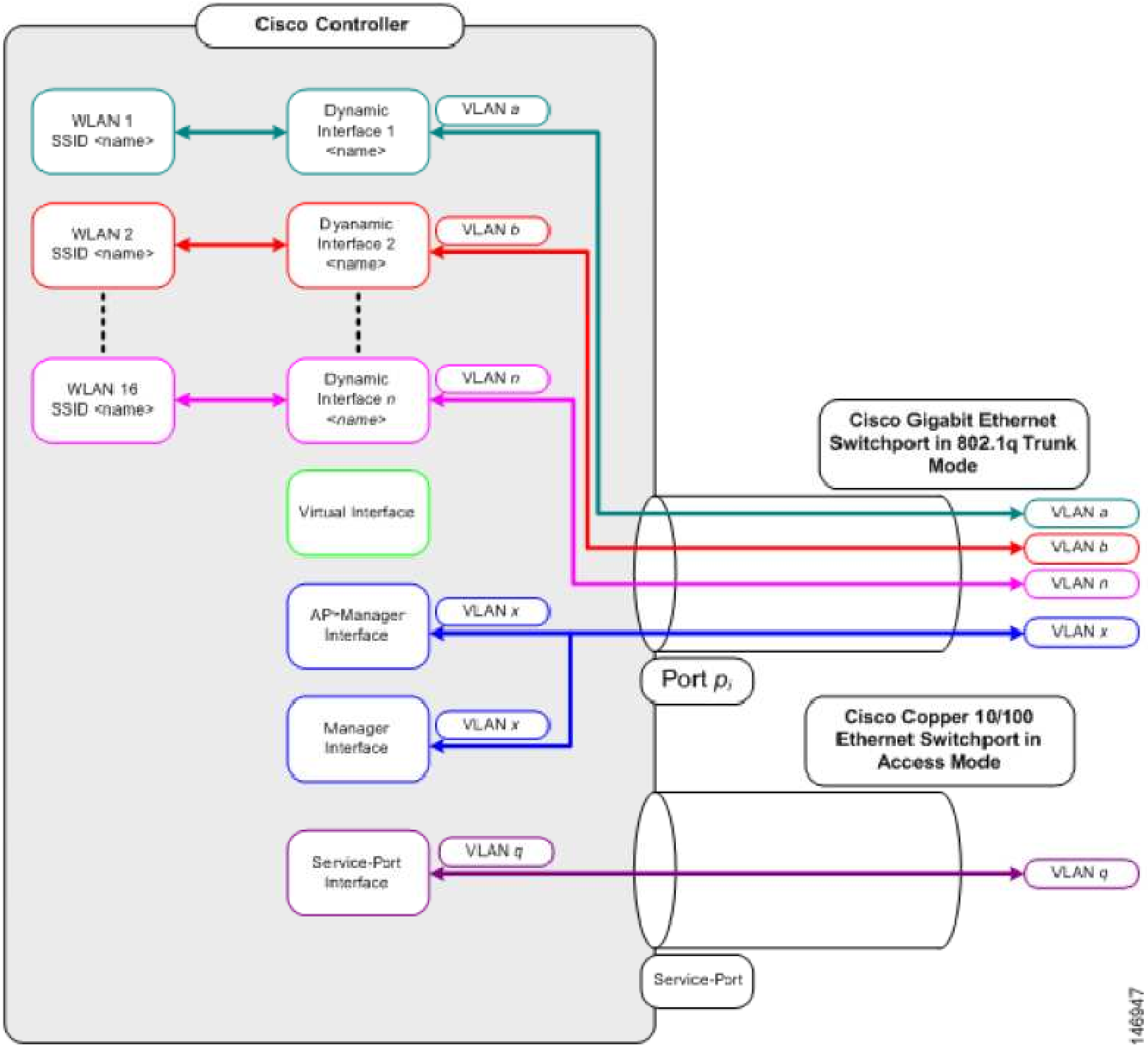
Despliegue de APs

- Prevenir el robo de APs
- Definir vlan de gestión
- Recomendable sistema centralizado
  - Gestión óptima de canales y potencia
  - Facilidad de despliegue de vlans y ssids
- Autenticar el AP
  - Certificado del AP
  - Punto protegido con 802.1X


Browser Based Remote Console for Cisco WCS
Third Party Integrated Applications: E911, Asset Tracking, ERP, Workflow Automation
Management Plane
Cisco Wireless Control System (WCS)
Cisco Wireless Location Appliance
Transmit Power
Interference Detection/Avoidance
Rogue Detection/Containment
RF Domain
Control Plane
Radio Resource Management Software
User Load Management
Coverage Hole Management
Automatic Channel Management
Mobility Management
LWAPP
Catalyst 6500 Series WiSM
Data Plane
WLAN Controller
LWAPP
LWAPP
REAP
Mesh Access Point
Small/Medium Office
Remote Office
Outdoor Environment

Configuraciones extra

- Obligatorio DHCP
  - El controler bloquea IPs estáticas
- No permitir tráfico entre los usuarios wifi
  - Juegos en red, propagación de bichos varios, etc…
  - Problemas: VoIP (streams udp directos) y otros P2P
- Opcional: Autenticar las tramas de gestión
  - Evitar Deauth Floods
  - Problema de compatibilidad


Cisco Controller
WLAN 1
SSID <name>
Dynamic
Interface 1
<name>
VLAN a
WLAN 2
SSID <name>
Dyanamic
Interface 2
<name>
VLAN b
WLAN 16
SSID <name>
Dynamic
Interface n
<name>
VLAN n
Virtual Interface
AP-Manager
Interface
VLAN x
Manager
Interface
VLAN x
Service-Port
Interface
VLAN q
Cisco Gigabit Ethernet
Switchport in 802.1q Trunk
Mode
VLAN a
VLAN b
VLAN n
VLAN x
Port p_i
Cisco Copper 10/100
Ethernet Switchport in
Access Mode
VLAN q
Service-Port
146947

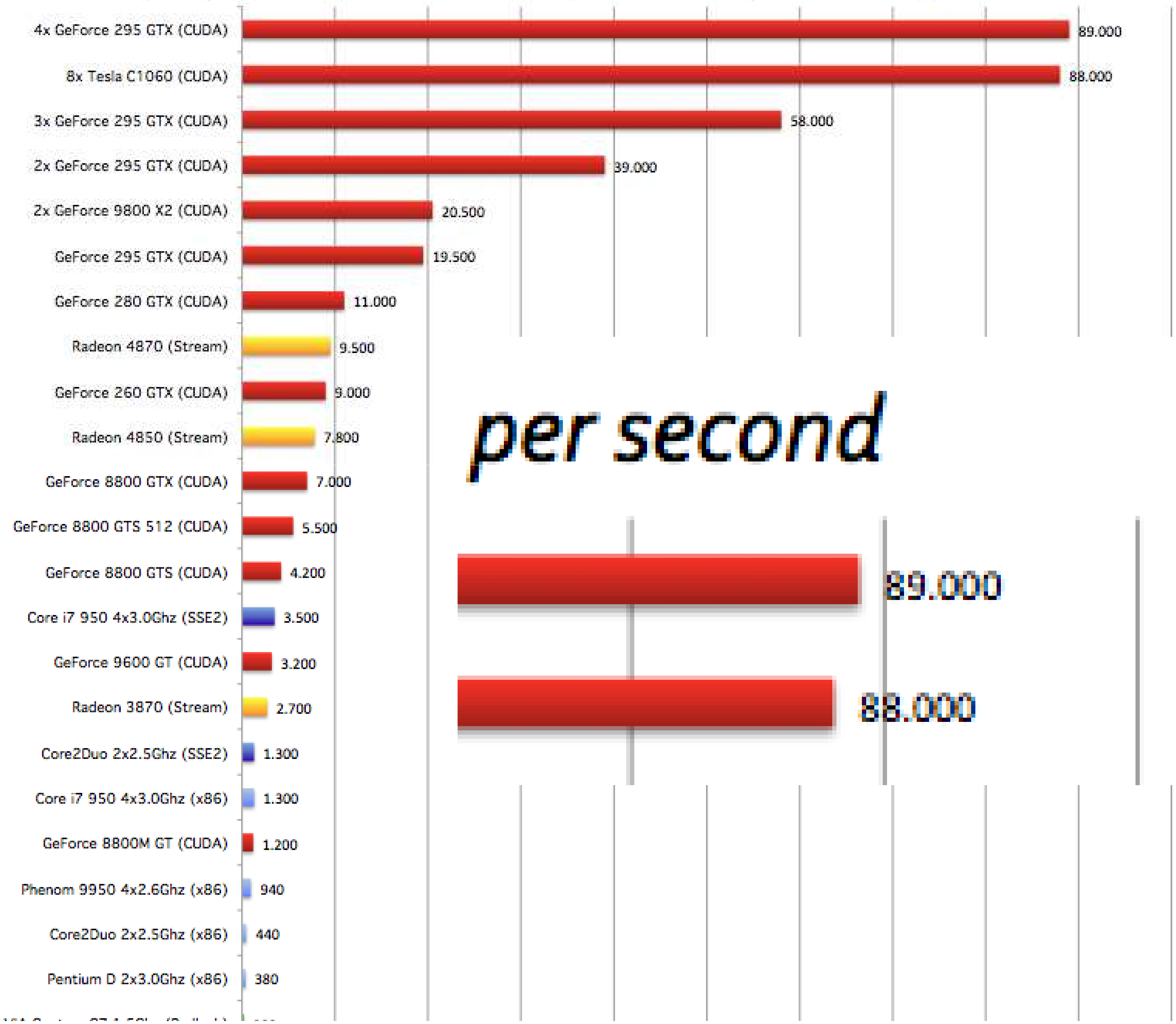
Despliegue de SSIDs

- Minimizar el número de SSIDs: Uno por acceso
  - Vlans dedicadas únicamente a wifi
  - SSID Open-Auth: Portal cautivo
    - Eventos
    - Intranet y manuales de configuración eduroam
  - SSID Eduroam: 802.1x
    - Único para todos los usuarios
    - Segmentar vlans PDI,ALU,etc… vía atributos RADIUS
    - Aprovechar los atributos para vpn, lan-802.1x, etc…

Autenticar usuarios

- Evitar el uso de PSK: si podemos…
  - Un secreto compartido no es un secreto
  - Con wep estamos perdidos
  - Con tkip es más teórico que práctico
  - Fuerza bruta contra la PMK (AES/TKIP)

Pyrit performing on various platforms - Computed PMKs per second



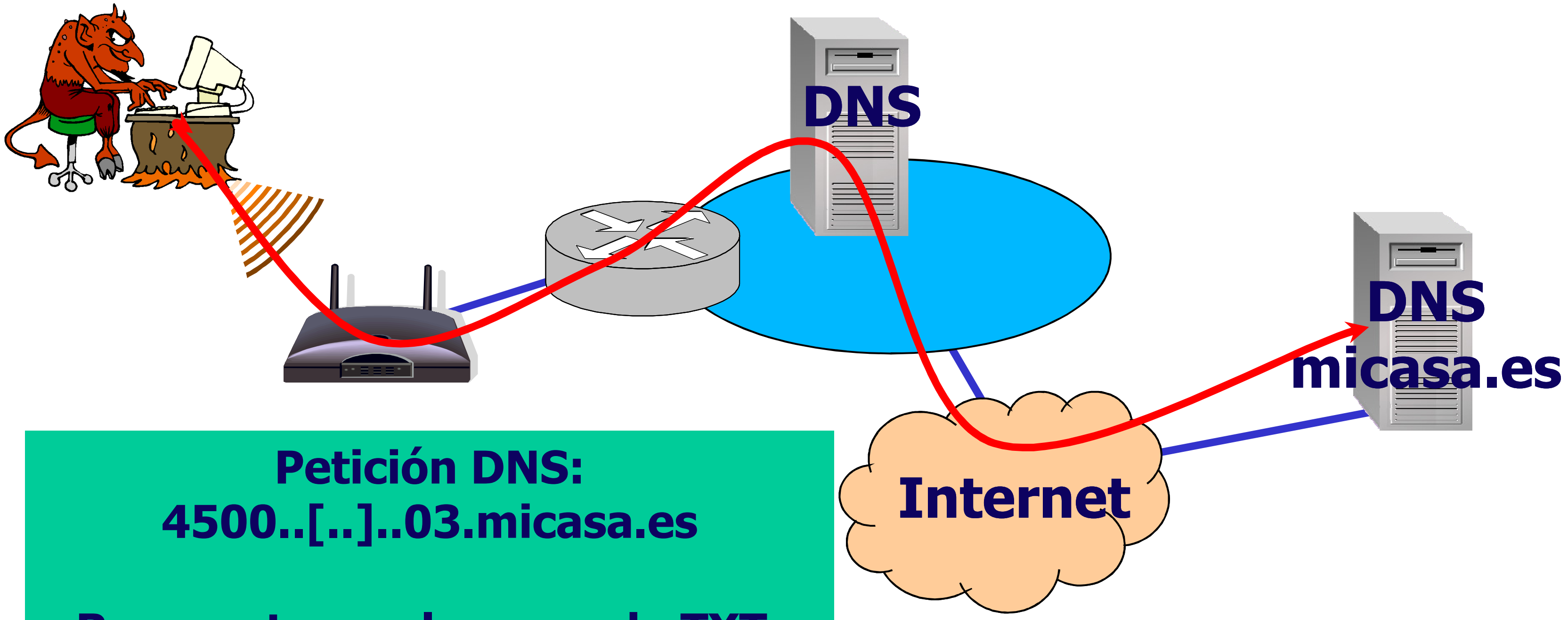
Autenticar usuarios

- 802.1x-Enterprise
  - Una vez configurado es lo mas práctico
  - Problemas:
    - Gestión y distribución de credenciales
    - El cliente decide si verifica el certificado del servidor
    - ¿Quién se atreve con TLS?

Autenticar usuarios

- Portal cautivo
  - Necesario
    - Eventos
    - Acceso a Intranet y manuales para activar servicio eduroam
    - Terminales no compatibles eduroam
  - ¿Cómo ciframos? Nivel 3: VPN/SSL-VPN?
- Ojo! DNS-Tunneling

DNS-Tunneling

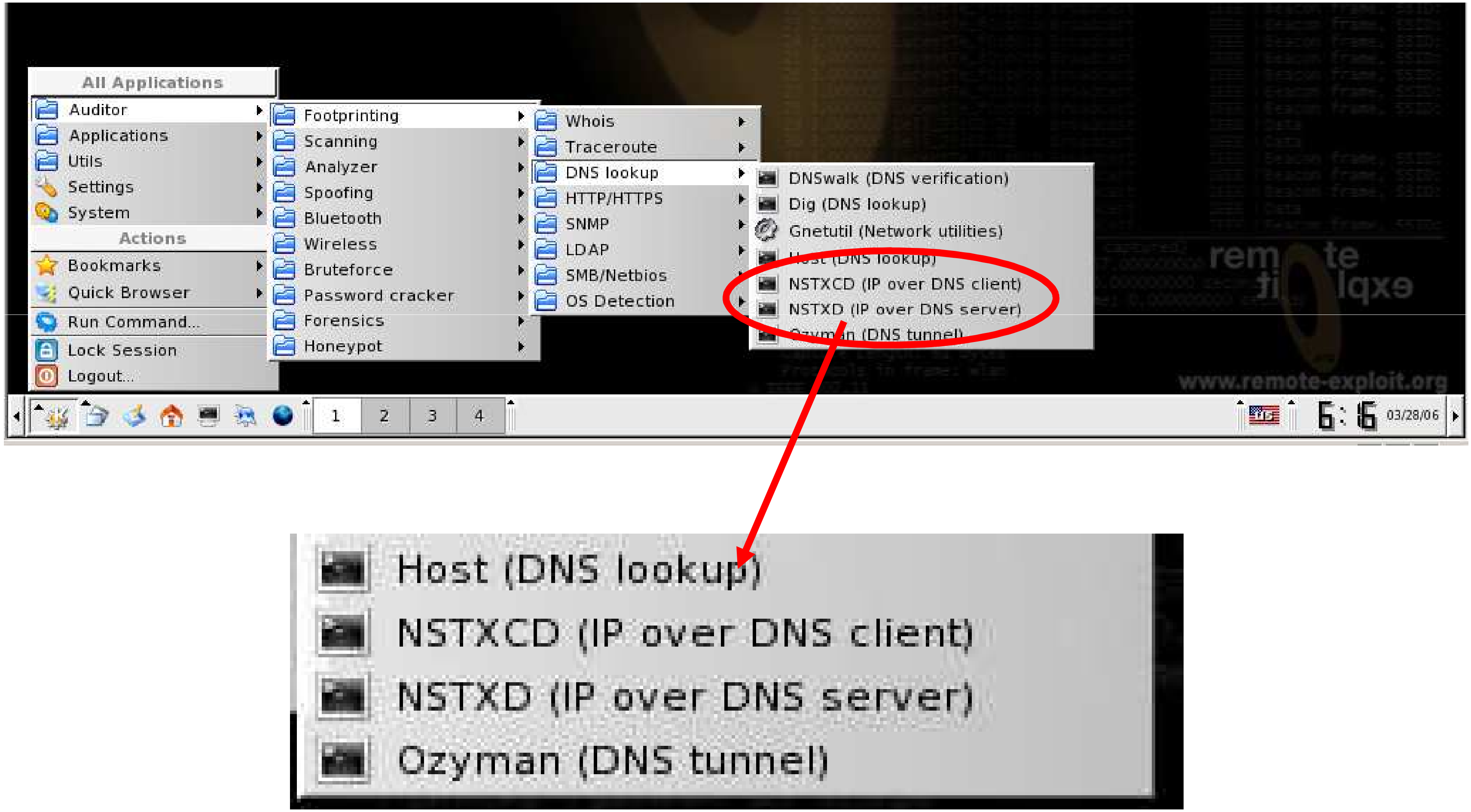


Petición DNS:
4500..[..]..03.micasa.es

Respuesta en el campo de TXT:
"45000...[..]..e6e5"

Paquetes IP!!!

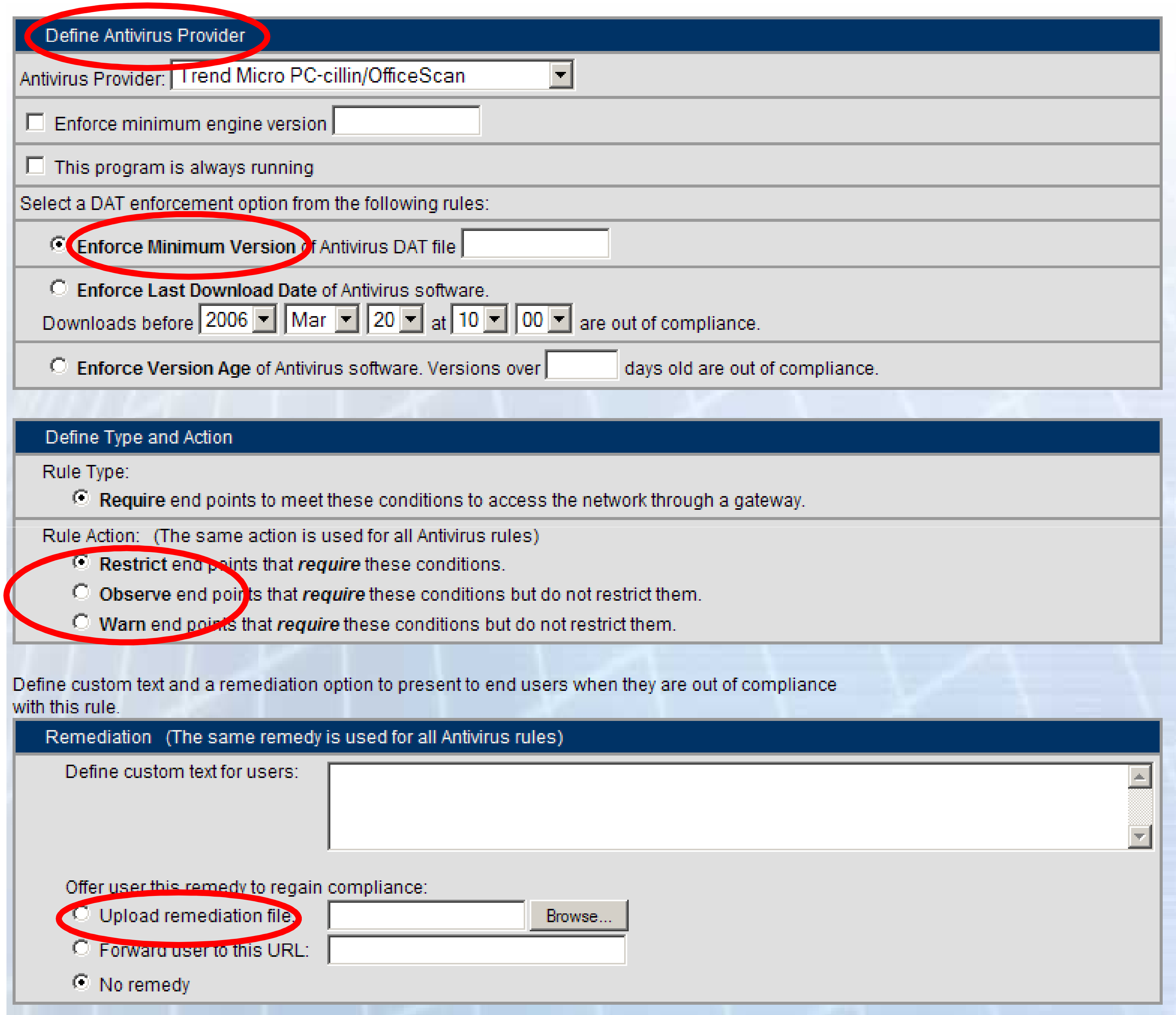
DNS-Tunneling



Control de admisión NAC

Arquitectura segura wifi

- NAC
  - Difícil con la diversidad de terminales
  - Alguna experiencia:



Define Antivirus Provider

Antivirus Provider: Trend Micro PC-cillin/OfficeScan

□ Enforce minimum engine version

□ This program is always running

Select a DAT enforcement option from the following rules:

● **Enforce Minimum Version** of Antivirus DAT file

○ **Enforce Last Download Date** of Antivirus software.
Downloads before 2006 Mar 20 at 10 00 are out of compliance.

○ **Enforce Version Age** of Antivirus software. Versions over days old are out of compliance.

Define Type and Action

Rule Type:

● **Require** end points to meet these conditions to access the network through a gateway.

Rule Action: (The same action is used for all Antivirus rules)

● **Restrict** end points that ***require*** these conditions.

○ **Observe** end points that ***require*** these conditions but do not restrict them.

○ **Warn** end points that ***require*** these conditions but do not restrict them.

Define custom text and a remediation option to present to end users when they are out of compliance with this rule.

Remediation (The same remedy is used for all Antivirus rules)

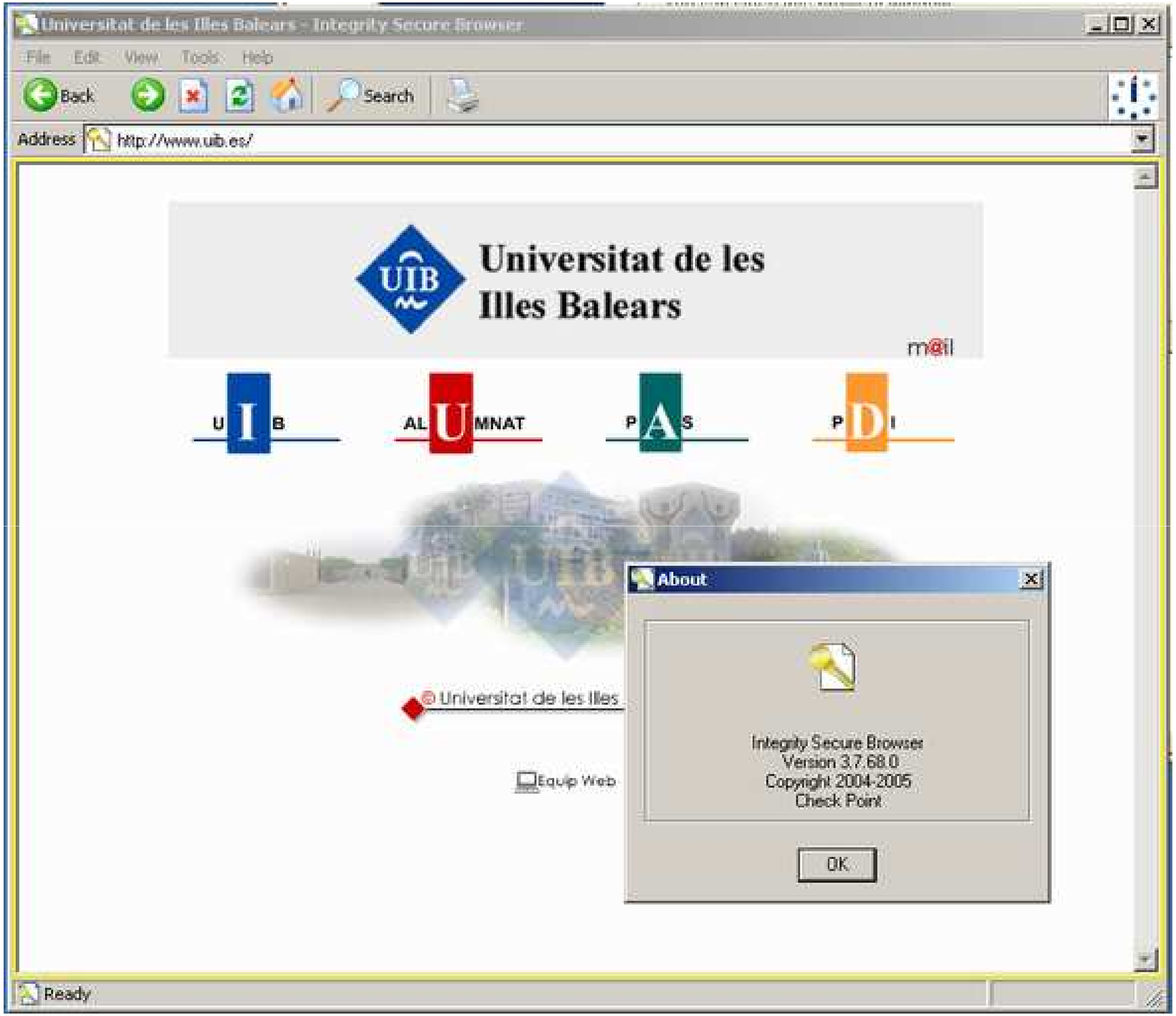
Define custom text for users:

Offer user this remedy to regain compliance:

○ Upload remediation file: Browse...

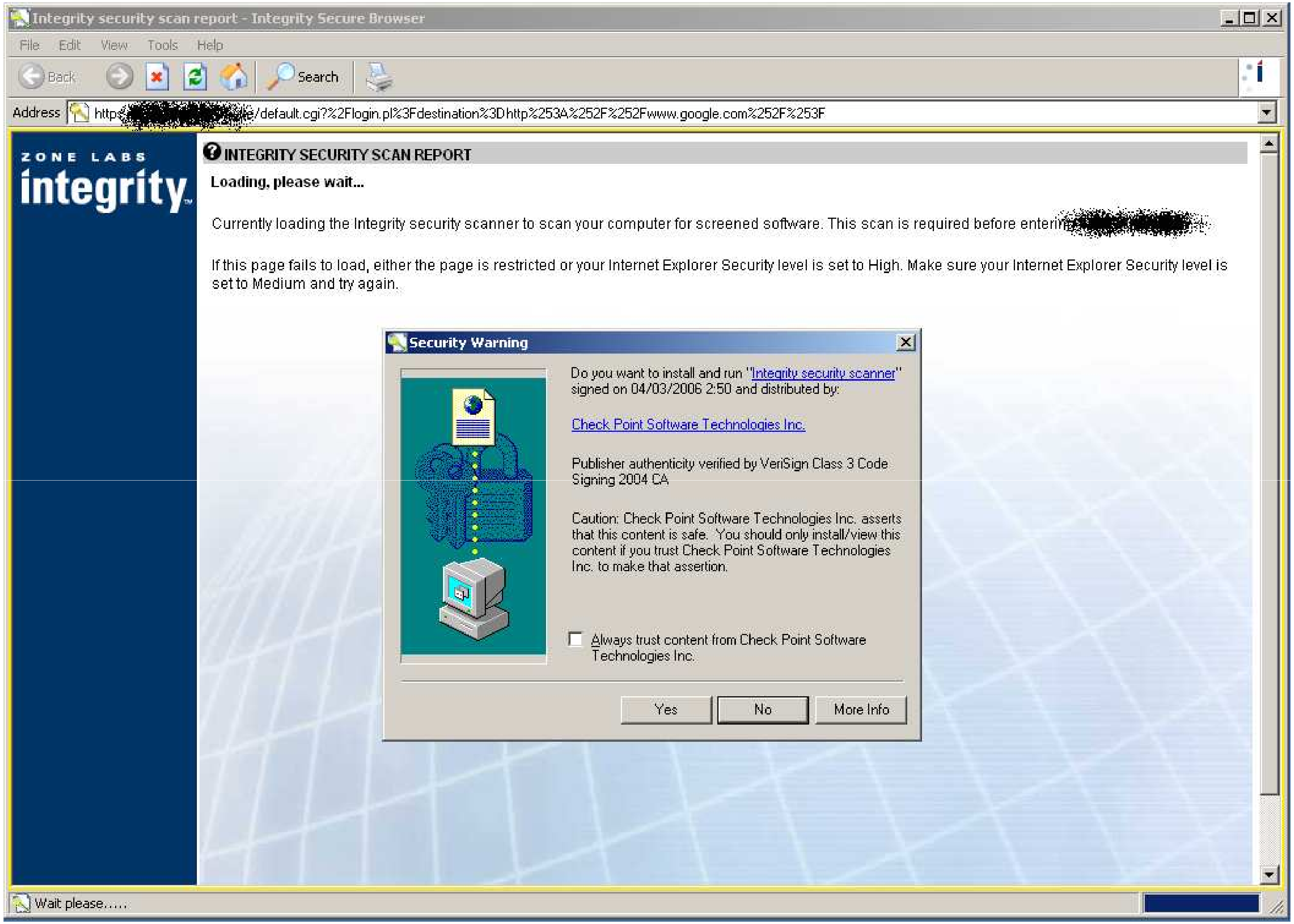
○ Forward user to this URL:

● No remedy



Universitat de les Illes Balears - Integrity Secure Browser
File Edit View Tools Help
Back
Search
Address
http://www.uib.es/
Universitat de les Illes Balears
m@il
U I B
AL U MNAT
P A S
P D I
© Universitat de les Illes
Equip Web
Ready
About
OK

Integrity Secure Browser
Version 3.7.68.0
Copyright 2004-2005
Check Point



http[redacted]/default.cgi?%2Flogin.pl%3Fdestination%3Dhttp%253A%252F%252Fwww.google.com%252F%253F

INTEGRITY SECURITY SCAN REPORT

Loading, please wait...

Currently loading the Integrity security scanner to scan your computer for screened software. This scan is required before enterin[redacted]

If this page fails to load, either the page is restricted or your Internet Explorer Security level is set to High. Make sure your Internet Explorer Security level is set to Medium and try again.

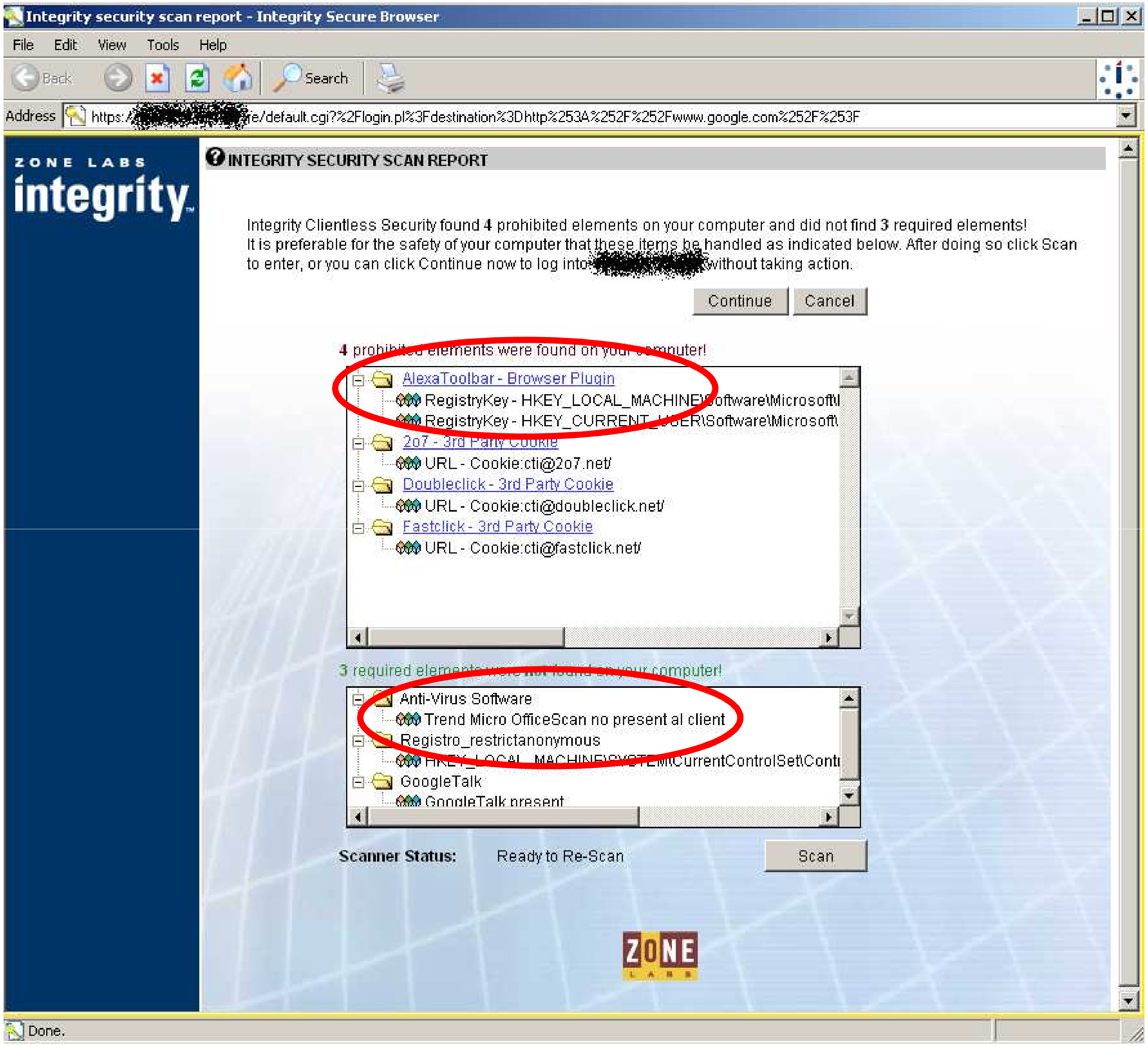
Do you want to install and run "Integrity security scanner" signed on 04/03/2006 2:50 and distributed by:

Check Point Software Technologies Inc.

Publisher authenticity verified by VeriSign Class 3 Code Signing 2004 CA

Caution: Check Point Software Technologies Inc. asserts that this content is safe. You should only install/view this content if you trust Check Point Software Technologies Inc. to make that assertion.

☐ Always trust content from Check Point Software Technologies Inc.


Integrity security scan report - Integrity Secure Browser
File Edit View Tools Help
Back
Search
Address
ZONE LABS
integrity
Continue
Cancel
Scan
ZONE LABS
Done.

https://[redacted]e/default.cgi?%2Flogin.pl%3Fdestination%3Dhttp%253A%252F%252Fwww.google.com%252F%253F

INTEGRITY SECURITY SCAN REPORT

Integrity Clientless Security found 4 prohibited elements on your computer and did not find 3 required elements! It is preferable for the safety of your computer that these items be handled as indicated below. After doing so click Scan to enter, or you can click Continue now to log into [redacted] without taking action.

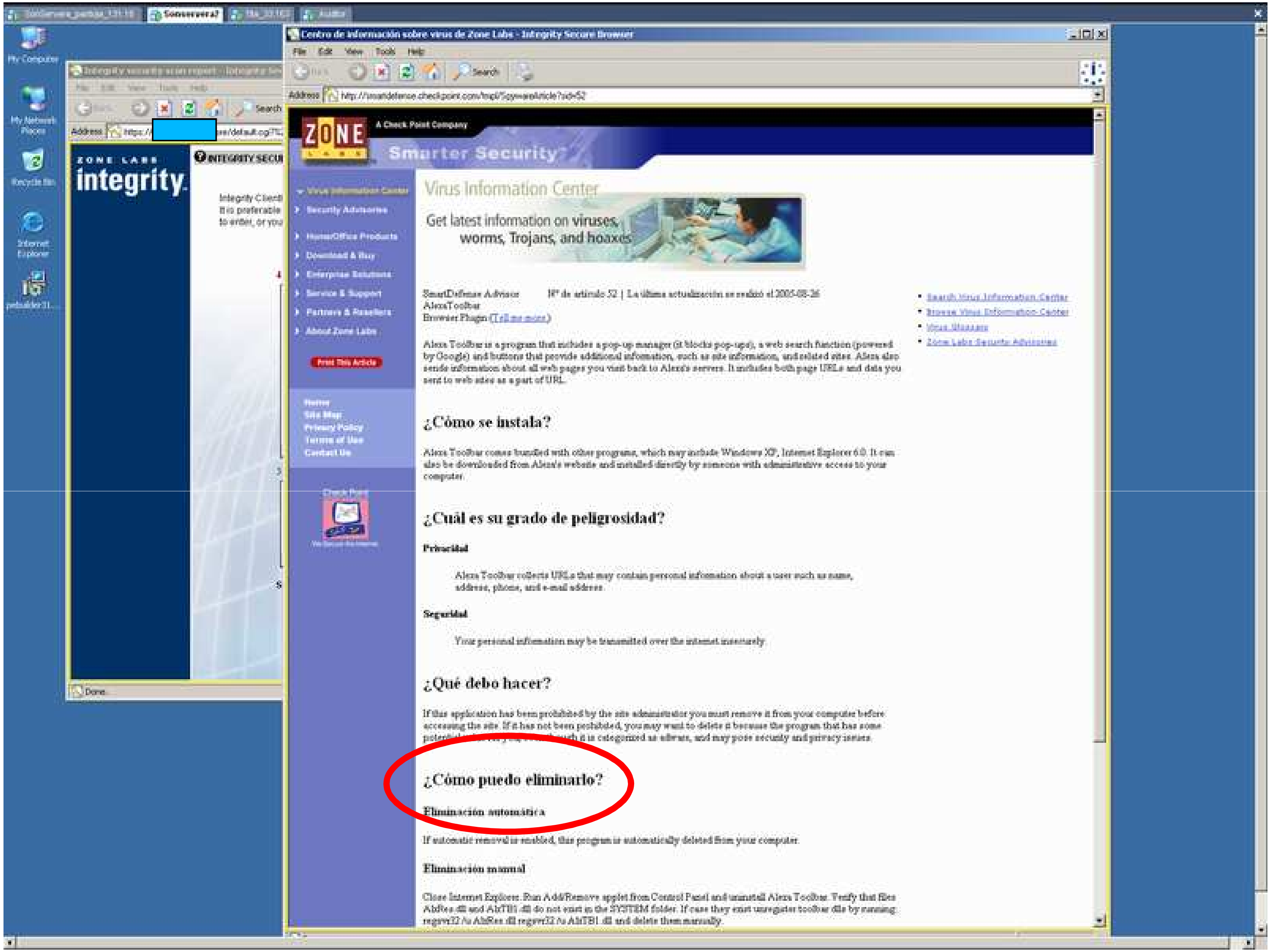
4 prohibited elements were found on your computer!

- AlexaToolbar - Browser Plugin
  - RegistryKey - HKEY_LOCAL_MACHINE\Software\Microsoft\I
  - RegistryKey - HKEY_CURRENT_USER\Software\Microsoft\
- 2o7 - 3rd Party Cookie
  - URL - Cookie:cti@2o7.net/
- Doubleclick - 3rd Party Cookie
  - URL - Cookie:cti@doubleclick.net/
- Fastclick - 3rd Party Cookie
  - URL - Cookie:cti@fastclick.net/

3 required elements were not found on your computer!

- Anti-Virus Software
  - Trend Micro OfficeScan no present al client
- Registro_restrictanonymous
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Contr
- GoogleTalk
  - GoogleTalk present

Scanner Status: Ready to Re-Scan



Virus Information Center

SmartDefense Advisor N° de artículo 52 | La última actualización se realizó el 2005-08-26
AlexaToolbar
Browser Plugin (Tell me more)

Alexa Toolbar is a program that includes a pop-up manager (it blocks pop-ups), a web search function (powered by Google) and buttons that provide additional information, such as site information, and related sites. Alexa also sends information about all web pages you visit back to Alexa's servers. It includes both page URLs and data you send to web sites as a part of URL.

¿Cómo se instala?

Alexa Toolbar comes bundled with other programs, which may include Windows XP, Internet Explorer 6.0. It can also be downloaded from Alexa's website and installed directly by someone with administrative access to your computer.

¿Cuál es su grado de peligrosidad?

Privacidad

Alexa Toolbar collects URLs that may contain personal information about a user such as name, address, phone, and e-mail address.

Seguridad

Your personal information may be transmitted over the internet insecurely.

¿Qué debo hacer?

If this application has been prohibited by the site administrator you must remove it from your computer before accessing the site. If it has not been prohibited, you may want to delete it because the program that has some potential [illegible] though it is categorized as adware, and may pose security and privacy issues.

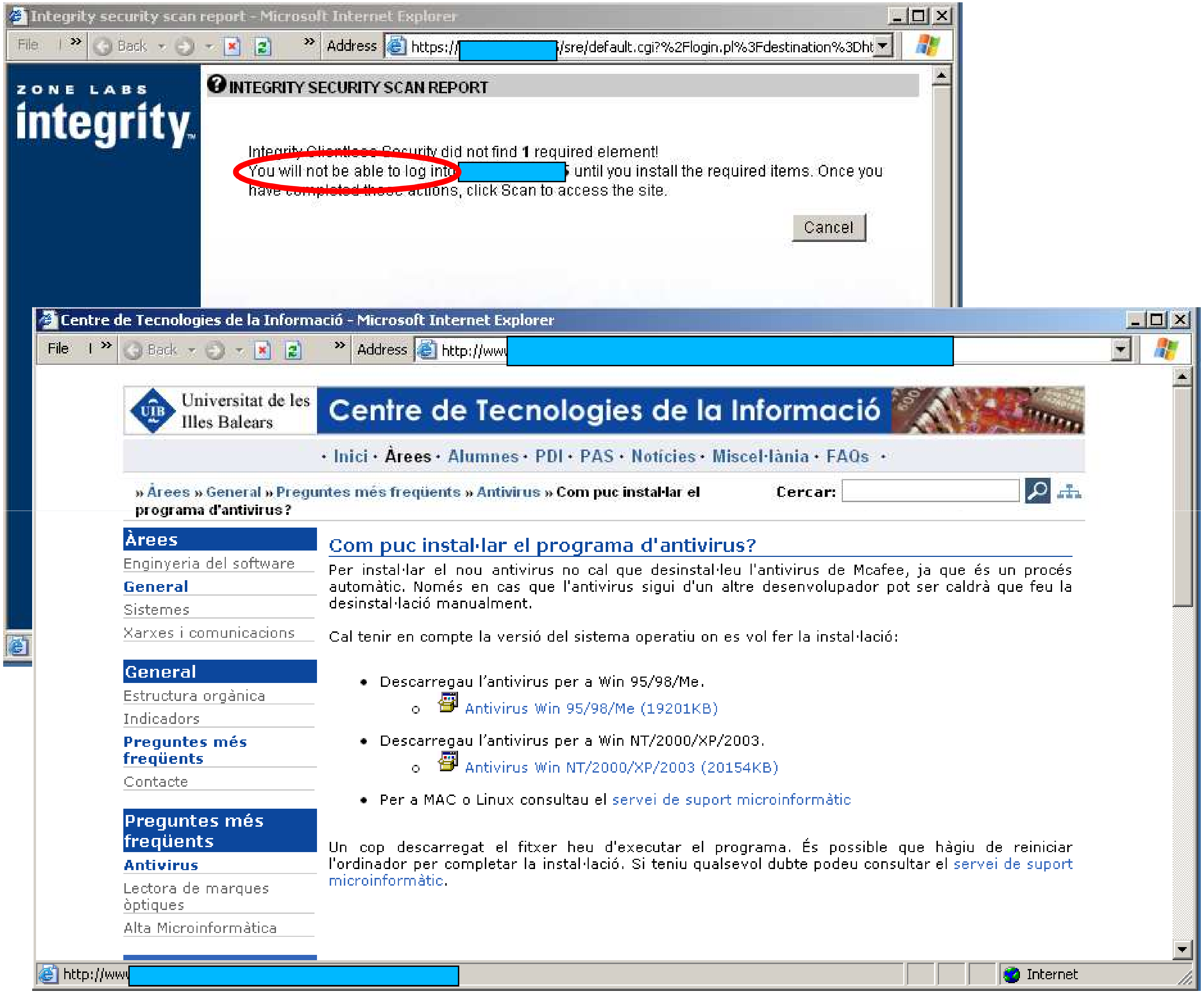
¿Cómo puedo eliminarlo?

Eliminación automática

If automatic removal is enabled, this program is automatically deleted from your computer.

Eliminación manual

Close Internet Explorer. Run Add/Remove applet from Control Panel and uninstall Alexa Toolbar. Verify that files AlxRes.dll and AlxTB1.dll do not exist in the SYSTEM folder. If case they exist unregister toolbar dlls by running regsvr32 /u AlxRes.dll regsvr32 /u AlxTB1.dll and delete them manually.


Integrity security scan report - Microsoft Internet Explorer
File
Back
Address
https://[redacted]/sre/default.cgi?%2Flogin.pl%3Fdestination%3Dht
ZONE LABS
integrity
Cancel
Centre de Tecnologies de la Informació - Microsoft Internet Explorer
Address
http://www[redacted]
Universitat de les Illes Balears
Centre de Tecnologies de la Informació
· Inici · Àrees · Alumnes · PDI · PAS · Notícies · Miscel·lània · FAQs ·
Cercar:
http://www[redacted]
Internet

INTEGRITY SECURITY SCAN REPORT

Integrity Clientless Security did not find 1 required element!
You will not be able to log into [redacted] until you install the required items. Once you have completed these actions, click Scan to access the site.

» Àrees » General » Preguntes més freqüents » Antivirus » Com puc instal·lar el programa d'antivirus?

Àrees
- Enginyeria del software
- General
- Sistemes
- Xarxes i comunicacions

General
- Estructura orgànica
- Indicadors
- Preguntes més freqüents
- Contacte

Preguntes més freqüents
- Antivirus
- Lectora de marques òptiques
- Alta Microinformàtica

Com puc instal·lar el programa d'antivirus?

Per instal·lar el nou antivirus no cal que desinstal·leu l'antivirus de Mcafee, ja que és un procés automàtic. Només en cas que l'antivirus sigui d'un altre desenvolupador pot ser caldrà que feu la desinstal·lació manualment.

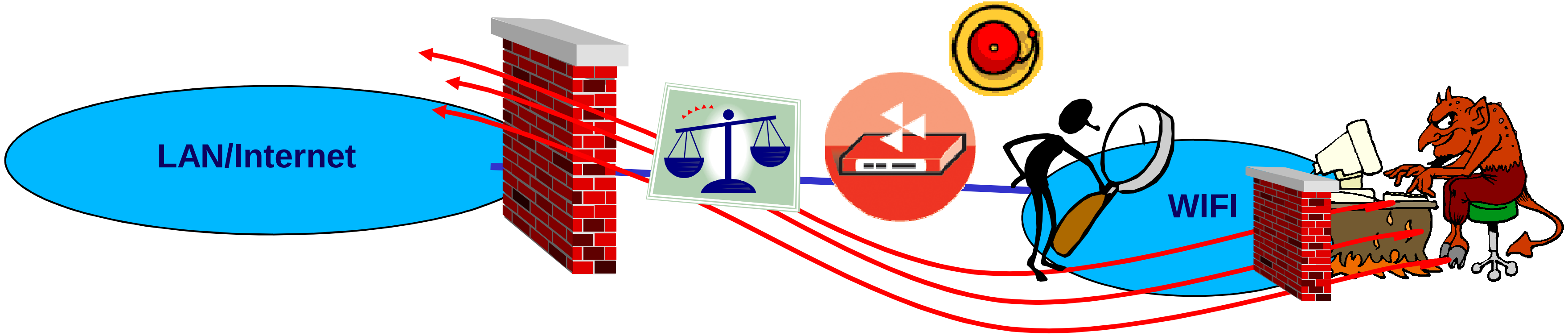
Cal tenir en compte la versió del sistema operatiu on es vol fer la instal·lació:

- Descarregau l'antivirus per a Win 95/98/Me.
  - Antivirus Win 95/98/Me (19201KB)
- Descarregau l'antivirus per a Win NT/2000/XP/2003.
  - Antivirus Win NT/2000/XP/2003 (20154KB)
- Per a MAC o Linux consultau el servei de suport microinformàtic

Un cop descarregat el fitxer heu d'executar el programa. És possible que hàgiu de reiniciar l'ordinador per completar la instal·lació. Si teniu qualsevol dubte podeu consultar el servei de suport microinformàtic.

Capas de análisis/filtrado

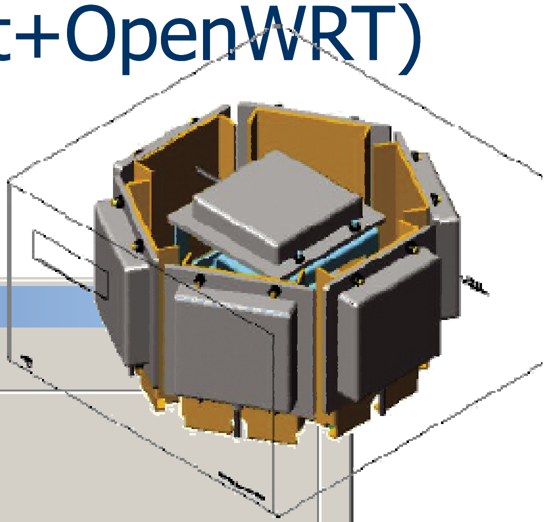
- Análisis/bloqueo de anomalías wifi (IDS/IDP)
- Políticas 802.1x vía atributos Radius
- Filtros de visibilidad: Firewall
- Análisis/bloqueo de anomalías IP (IDS/IDP)
- Gestión de ancho de banda

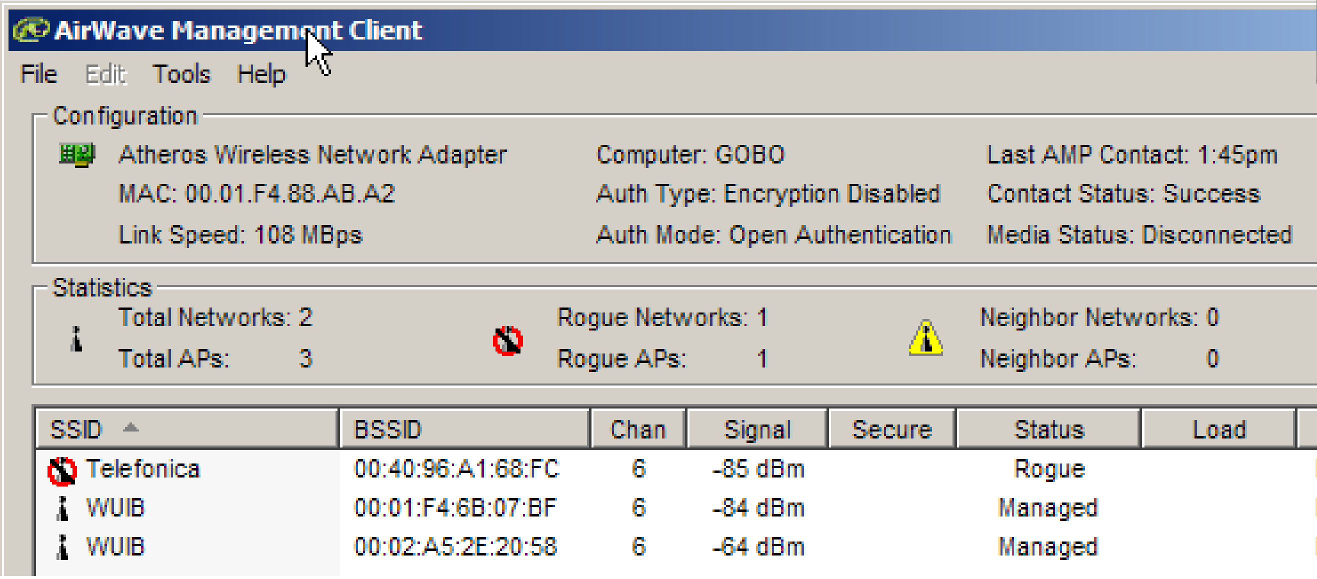


Red de Sensores

Arquitectura segura wifi

- Los APs y los clientes: son sensores
- Podemos construir sensores (Kismet+OpenWRT)
- Podemos comprar sensores





Configuration

Atheros Wireless Network Adapter
MAC: 00.01.F4.88.AB.A2
Link Speed: 108 MBps

Computer: GOBO
Auth Type: Encryption Disabled
Auth Mode: Open Authentication

Last AMP Contact: 1:45pm
Contact Status: Success
Media Status: Disconnected

Statistics

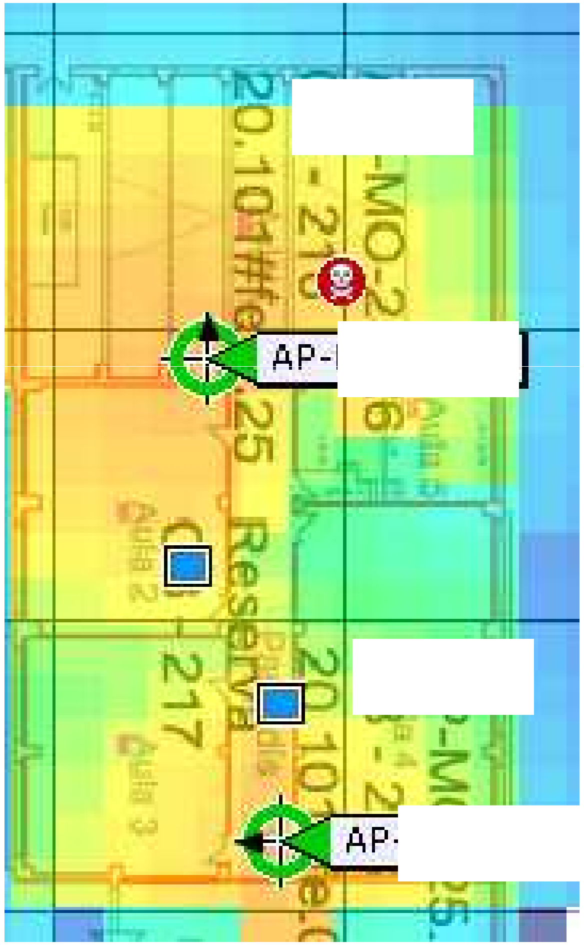
Total Networks: 2
Total APs: 3

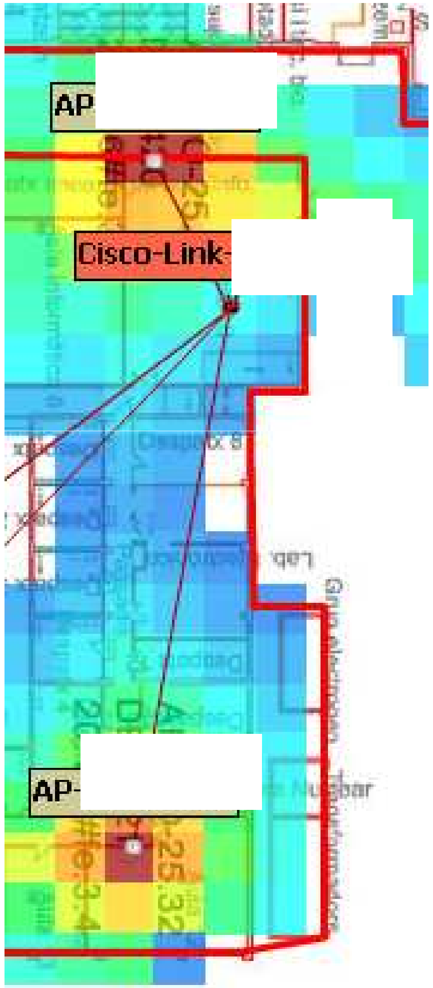
Rogue Networks: 1
Rogue APs: 1

Neighbor Networks: 0
Neighbor APs: 0

SSID	BSSID	Chan	Signal	Secure	Status	Load	Mode	Name
Telefonica	00:40:96:A1:68:FC	6	-85 dBm		Rogue		Infrastructure	
WUIB	00:01:F4:6B:07:BF	6	-84 dBm		Managed		Infrastructure	CTI1
WUIB	00:02:A5:2E:20:58	6	-64 dBm		Managed		Infrastructure	CTI6

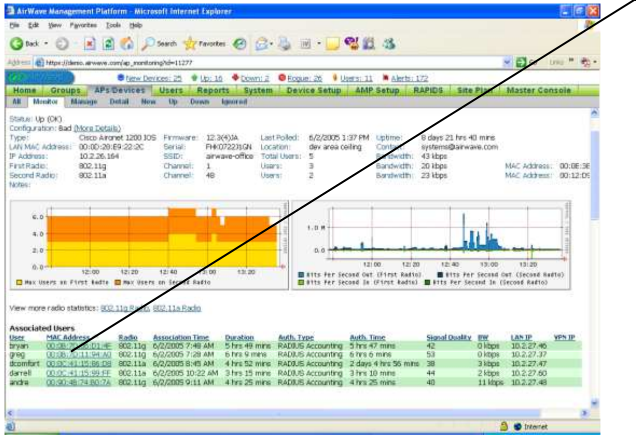
Localización de amenazas





Identificación de usuarios

Amenazas



AirWave Management Platform - Microsoft Internet Explorer

Address: https://demo.airwave.com/ap_monitoring?id=11277

New Devices: 25 · Up: 16 · Down: 2 · Rogue: 26 · Users: 11 · Alerts: 172

Status: Up (OK)
Configuration: Bad (More Details)

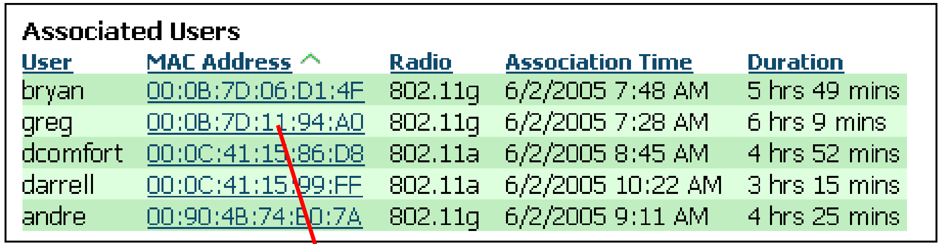
Type:	Cisco Aironet 1200 IOS	Firmware:	12.3(4)JA	Last Polled:	6/2/2005 1:37 PM	Uptime:	8 days 21 hrs 40 mins		
LAN MAC Address:	00:0D:28:E9:22:2C	Serial:	FHK0722J1GN	Location:	dev area ceiling	Contact:	systems@airwave.com		
IP Address:	10.2.26.164	SSID:	airwave-office	Total Users:	5	Bandwidth:	43 kbps		
First Radio:	802.11g	Channel:	1	Users:	3	Bandwidth:	20 kbps	MAC Address:	00:0E:3E
Second Radio:	802.11a	Channel:	48	Users:	2	Bandwidth:	23 kbps	MAC Address:	00:12:D9
Notes:									

6.0
4.0
2.0
0.0
12:00
12:20
12:40
13:00
13:20
Max Users on First Radio
Max Users on Second Radio
1.0 M
0.0
Bits Per Second Out (First Radio)
Bits Per Second Out (Second Radio)
Bits Per Second In (First Radio)
Bits Per Second In (Second Radio)

View more radio statistics: 802.11g Radio, 802.11a Radio

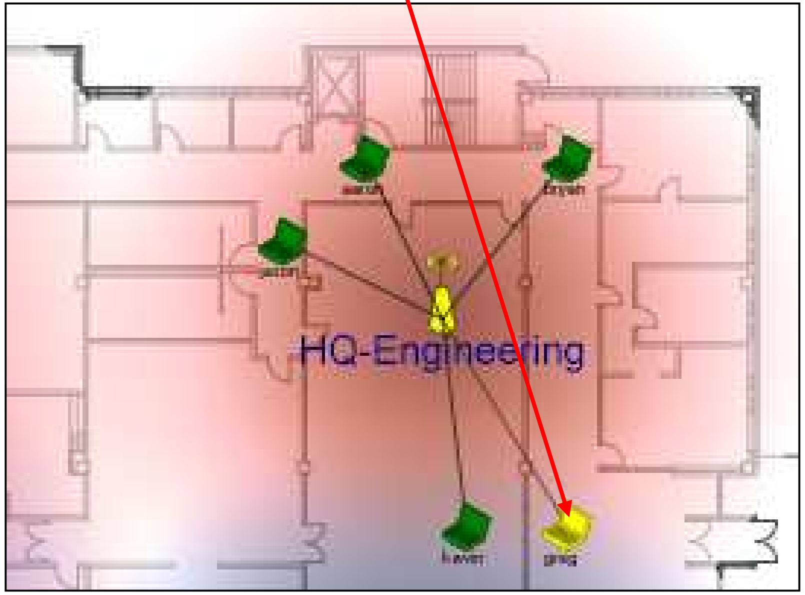
Associated Users

User	MAC Address	Radio	Association Time	Duration	Auth. Type	Auth. Time	Signal Quality	BW	LAN IP	VPN IP
bryan	00:0B:7D:06:D1:4F	802.11g	6/2/2005 7:48 AM	5 hrs 49 mins	RADIUS Accounting	5 hrs 47 mins	42	0 kbps	10.2.27.46	
greg	00:0B:7D:11:94:A0	802.11g	6/2/2005 7:28 AM	6 hrs 9 mins	RADIUS Accounting	6 hrs 6 mins	53	0 kbps	10.2.27.37	
dcomfort	00:0C:41:15:86:D8	802.11a	6/2/2005 8:45 AM	4 hrs 52 mins	RADIUS Accounting	2 days 4 hrs 56 mins	38	3 kbps	10.2.27.47	
darrell	00:0C:41:15:99:FF	802.11a	6/2/2005 10:22 AM	3 hrs 15 mins	RADIUS Accounting	3 hrs 10 mins	44	2 kbps	10.2.27.60	
andre	00:90:4B:74:B0:7A	802.11g	6/2/2005 9:11 AM	4 hrs 25 mins	RADIUS Accounting	4 hrs 25 mins	40	11 kbps	10.2.27.48	



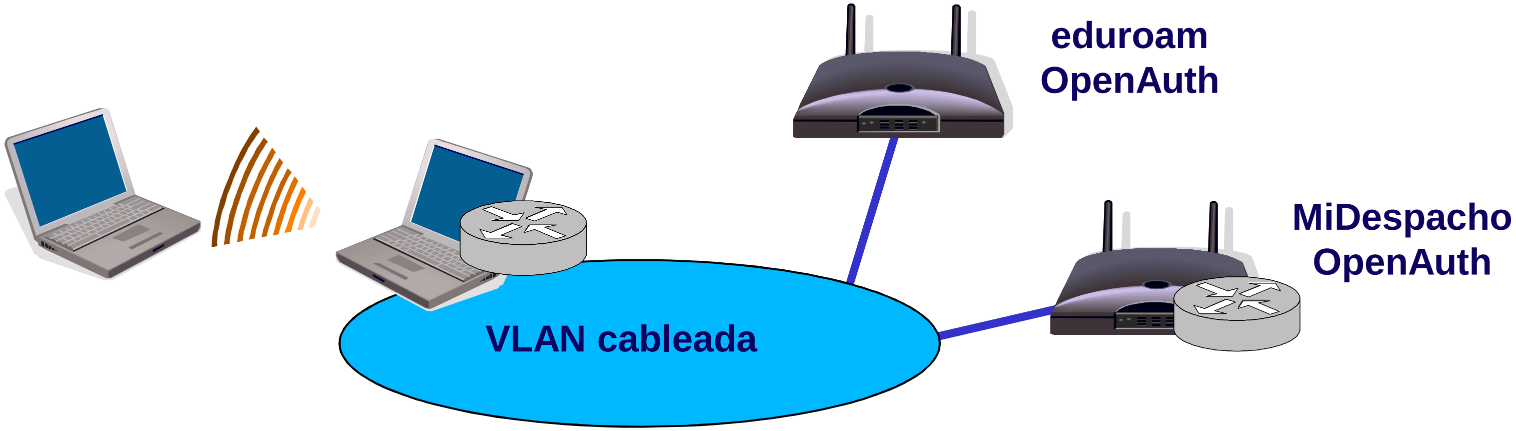
Associated Users

User	MAC Address	Radio	Association Time	Duration
bryan	00:0B:7D:06:D1:4F	802.11g	6/2/2005 7:48 AM	5 hrs 49 mins
greg	00:0B:7D:11:94:A0	802.11g	6/2/2005 7:28 AM	6 hrs 9 mins
dcomfort	00:0C:41:15:86:D8	802.11a	6/2/2005 8:45 AM	4 hrs 52 mins
darrell	00:0C:41:15:99:FF	802.11a	6/2/2005 10:22 AM	3 hrs 15 mins
andre	00:90:4B:74:B0:7A	802.11g	6/2/2005 9:11 AM	4 hrs 25 mins

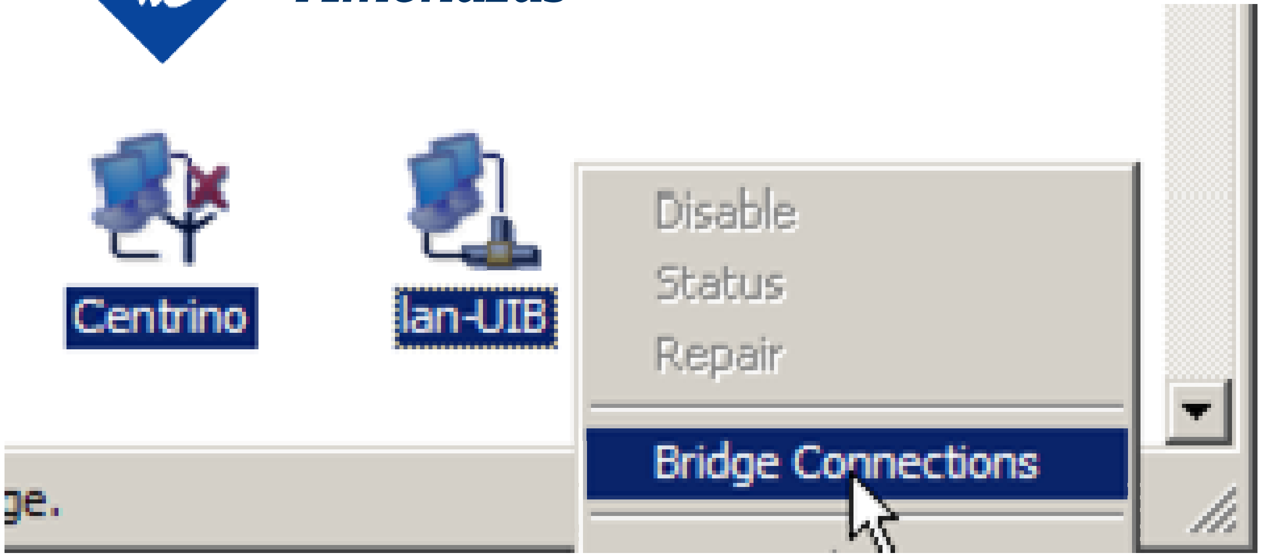


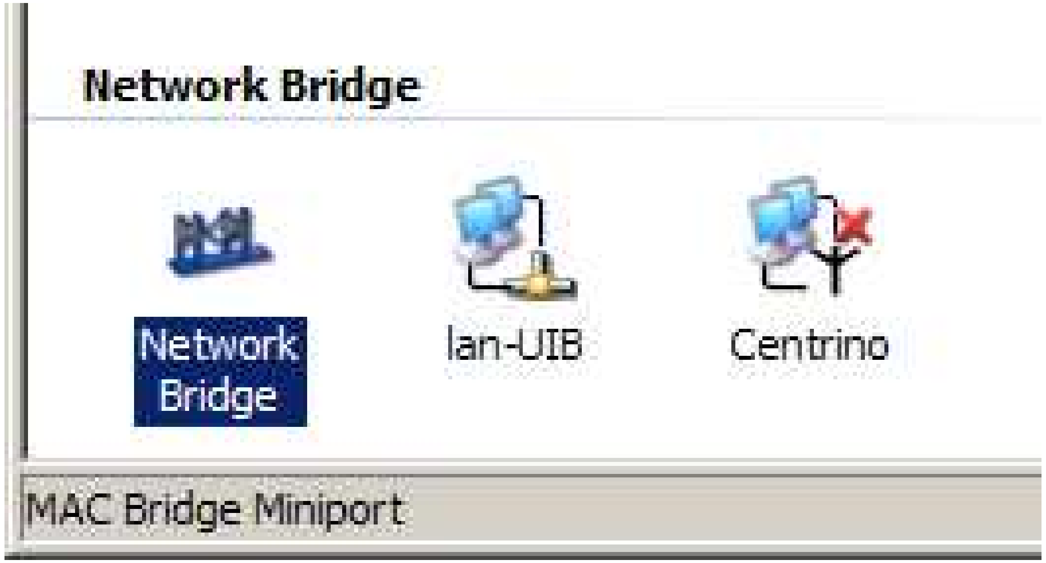
Rouge APs

- Rouge AP en vlan cableada
  - Bridge: Un AP en la LAN
  - Router: Un router-wifi en la LAN
  - PC de usuario en modo bridge/router



Usuario Bridge/Router



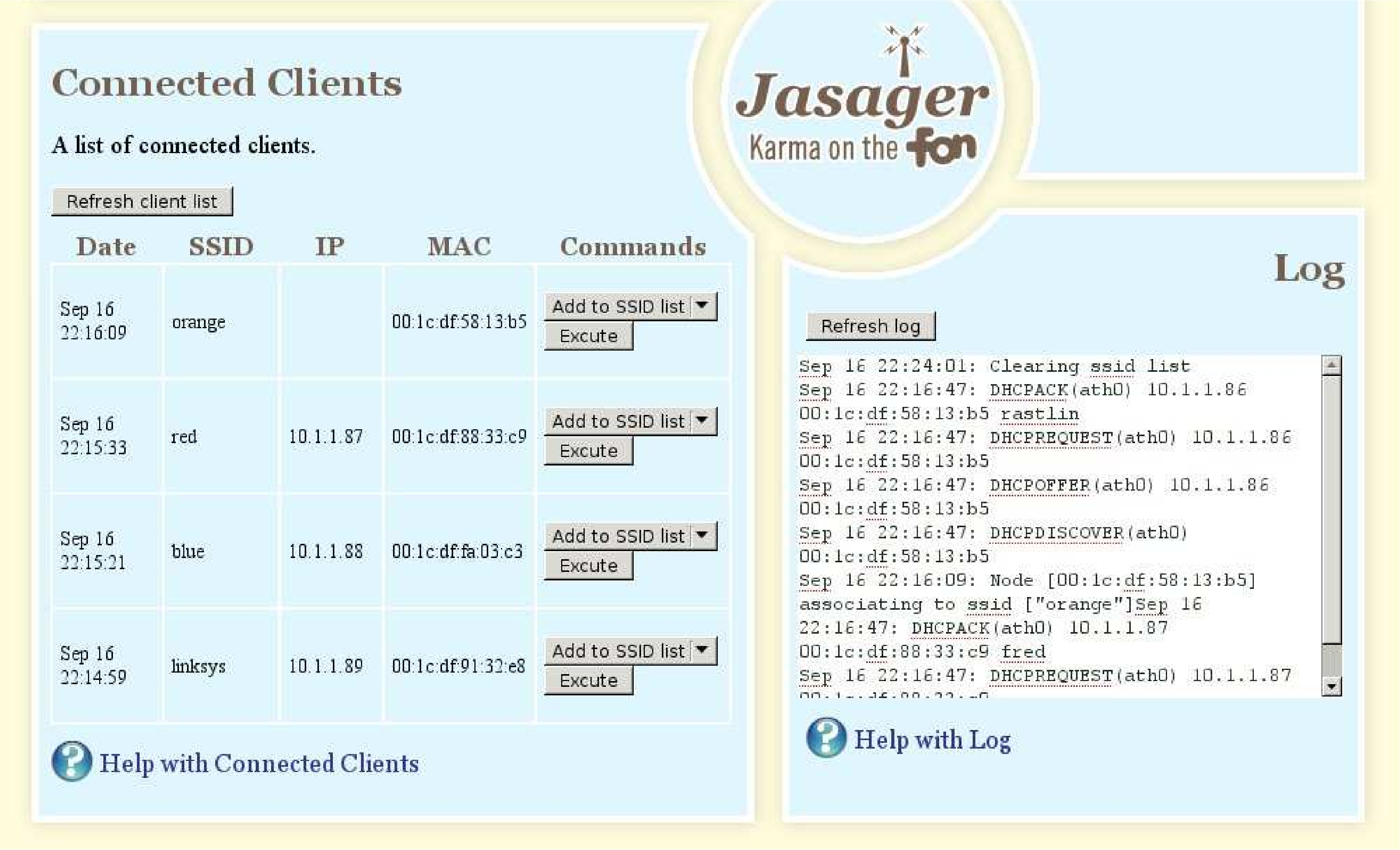


Suplantación del Portal cautivo

Amenazas

- Robo de credenciales
  - Usuarios que no verifican el certificado
  - Gran problema: unificar servicios/credenciales (SIR)
- Captura de tráfico

Suplantación de SSIDs



Connected Clients

A list of connected clients.

Refresh client list

Date	SSID	IP	MAC	Commands
Sep 16 22:16:09	orange		00:1c:df:58:13:b5	Add to SSID list ▾ Excute
Sep 16 22:15:33	red	10.1.1.87	00:1c:df:88:33:c9	Add to SSID list ▾ Excute
Sep 16 22:15:21	blue	10.1.1.88	00:1c:df:fa:03:c3	Add to SSID list ▾ Excute
Sep 16 22:14:59	linksys	10.1.1.89	00:1c:df:91:32:e8	Add to SSID list ▾ Excute

Help with Connected Clients

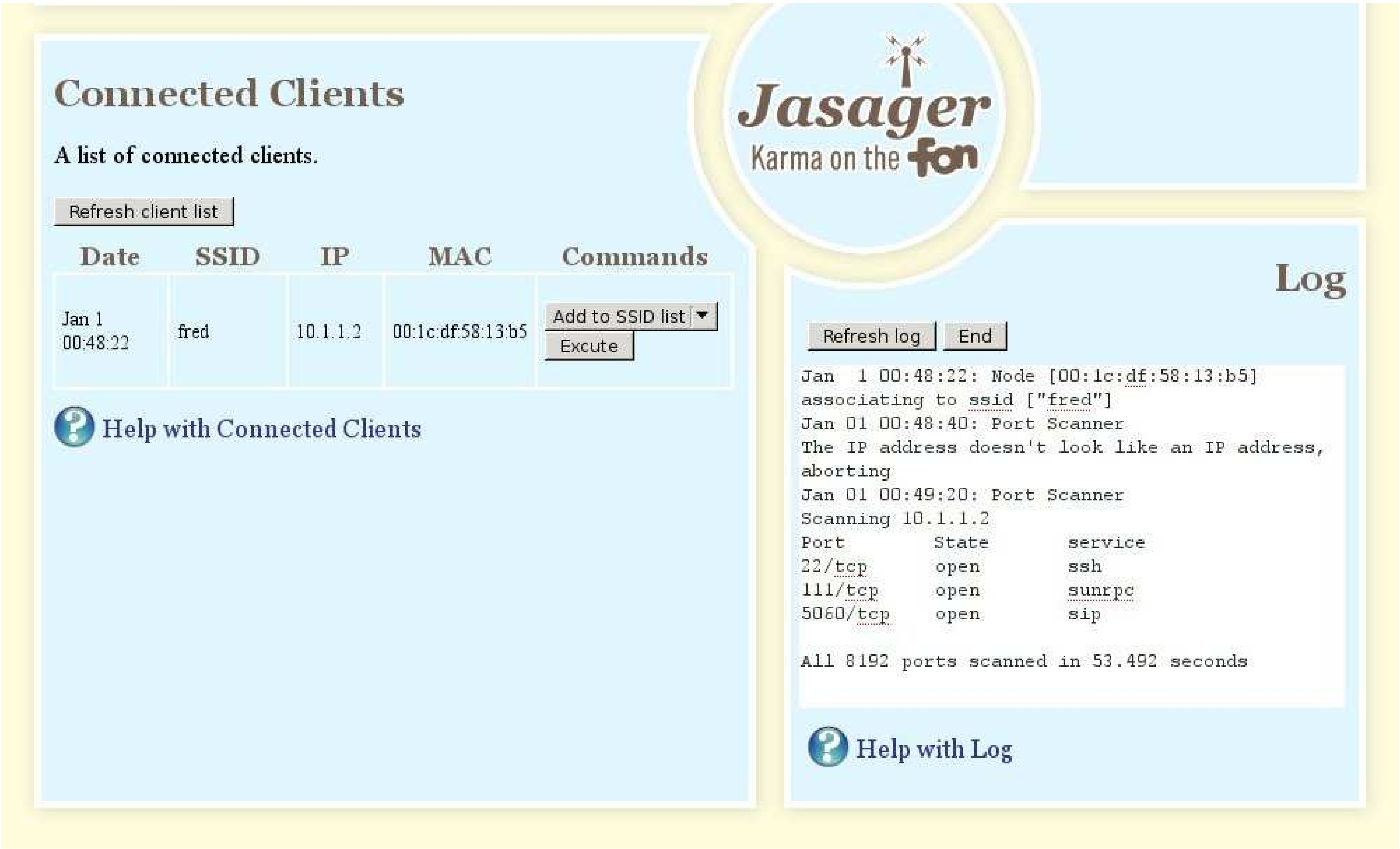
Log

Refresh log

```
Sep 16 22:24:01: Clearing ssid list
Sep 16 22:16:47: DHCPACK(ath0) 10.1.1.86
00:1c:df:58:13:b5 rastlin
Sep 16 22:16:47: DHCPREQUEST(ath0) 10.1.1.86
00:1c:df:58:13:b5
Sep 16 22:16:47: DHCPOFFER(ath0) 10.1.1.86
00:1c:df:58:13:b5
Sep 16 22:16:47: DHCPDISCOVER(ath0)
00:1c:df:58:13:b5
Sep 16 22:16:09: Node [00:1c:df:58:13:b5]
associating to ssid ["orange"]Sep 16
22:16:47: DHCPACK(ath0) 10.1.1.87
00:1c:df:88:33:c9 fred
Sep 16 22:16:47: DHCPREQUEST(ath0) 10.1.1.87
```

Help with Log

Suplantación de SSIDs



Connected Clients

A list of connected clients.

Date	SSID	IP	MAC	Commands
Jan 1 00:48:22	fred	10.1.1.2	00:1c:df:58:13:b5	Add to SSID list Excute

Help with Connected Clients

Log

```
Jan  1 00:48:22: Node [00:1c:df:58:13:b5]
associating to ssid ["fred"]
Jan 01 00:48:40: Port Scanner
The IP address doesn't look like an IP address,
aborting
Jan 01 00:49:20: Port Scanner
Scanning 10.1.1.2
Port        State       service
22/tcp      open        ssh
111/tcp     open        sunrpc
5060/tcp    open        sip

All 8192 ports scanned in 53.492 seconds
```

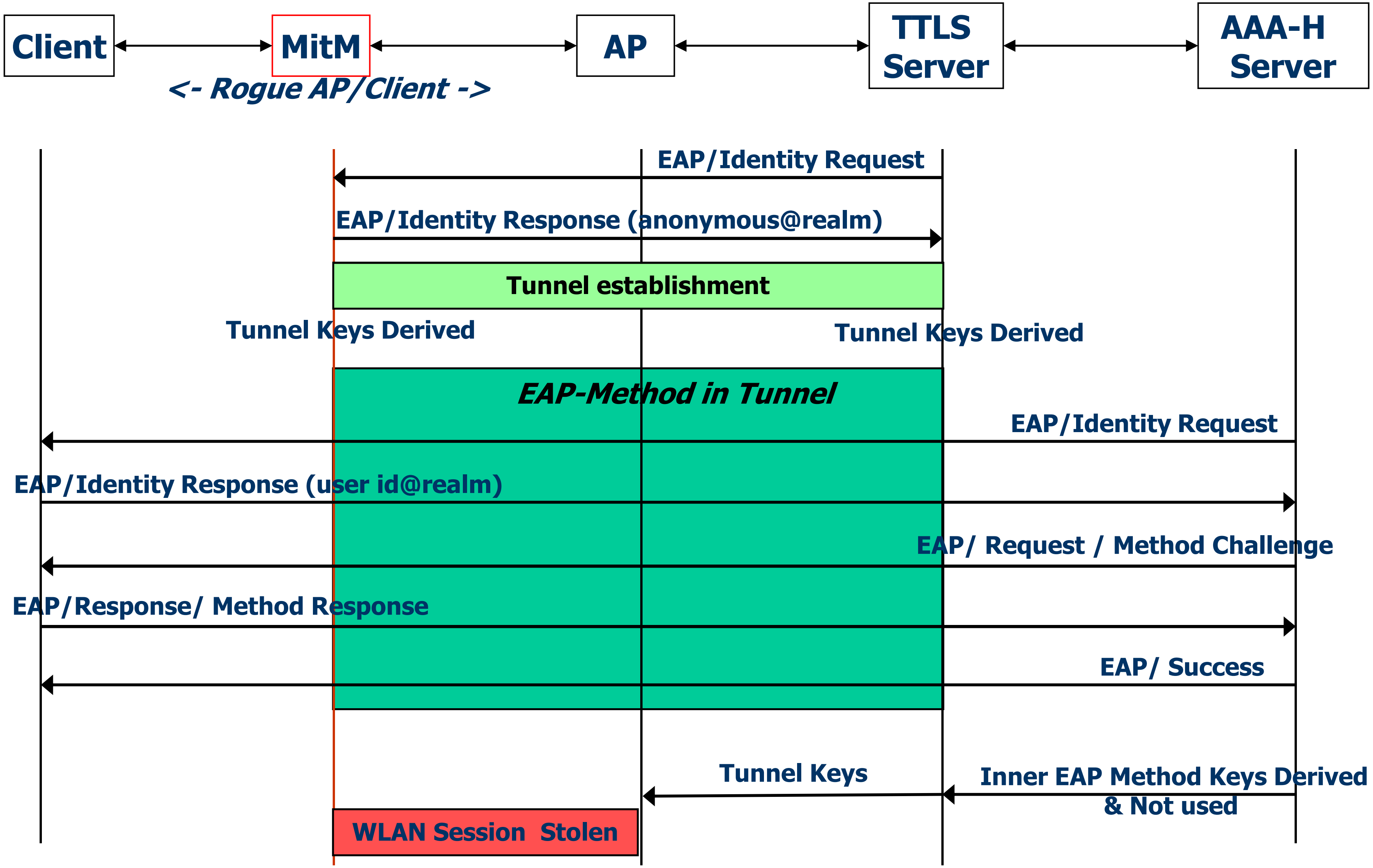
Help with Log

Suplantación de AP/Radius

- Robo de credenciales (TTLS/PAP)
  - El usuario decide si verifica o no el certificado
- Robo de sesiones
  - Es más teórico que práctico

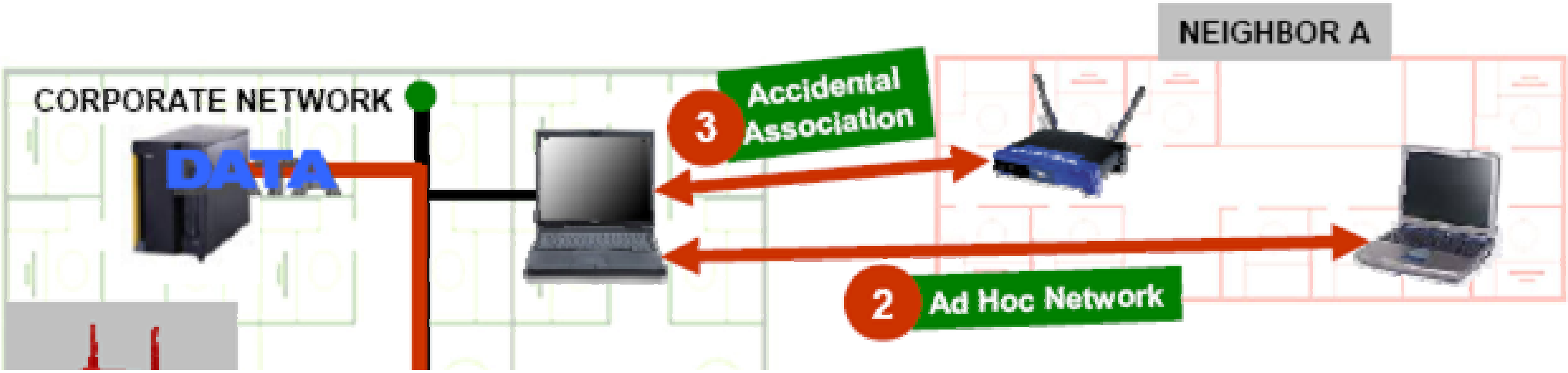
Robo de sesión/credenciales

Amenazas



Conexión a vecinos

- Terminales cableados conectados a vecinos wifi



Cifra tráfico hacia el portal

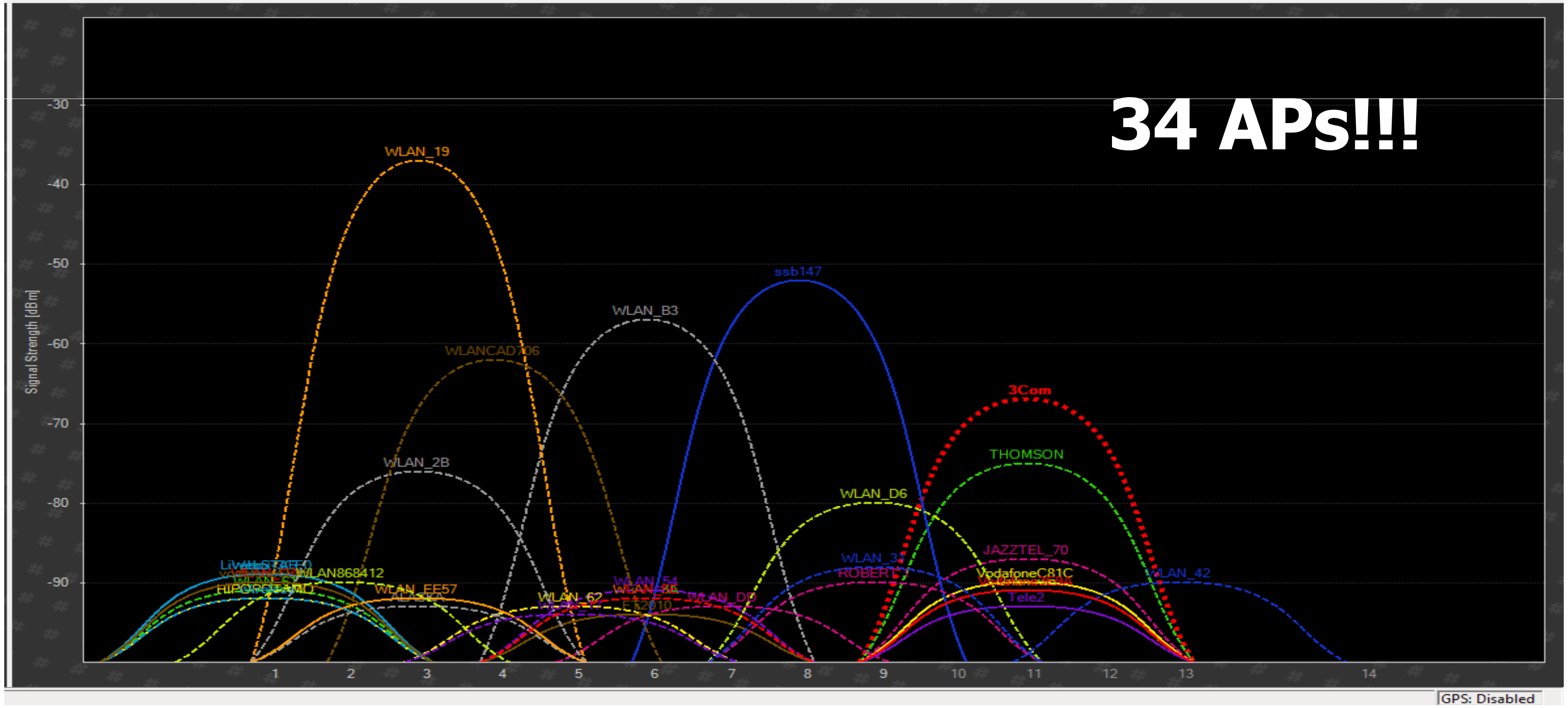
- Confidencialidad en los accesos vía portal
  - Solución de nivel 3: VPN/SSL-VPN
  - ¿Compatibilidad con todos los terminales…?

DoS nivel 2

- Disponibilidad: nivel 2
  - DoS a nivel 2: Deauth floods
    - MFP: Management Frame Protection
    - ¿Queremos asegurar la compatibilidad?

DoS nivel 1

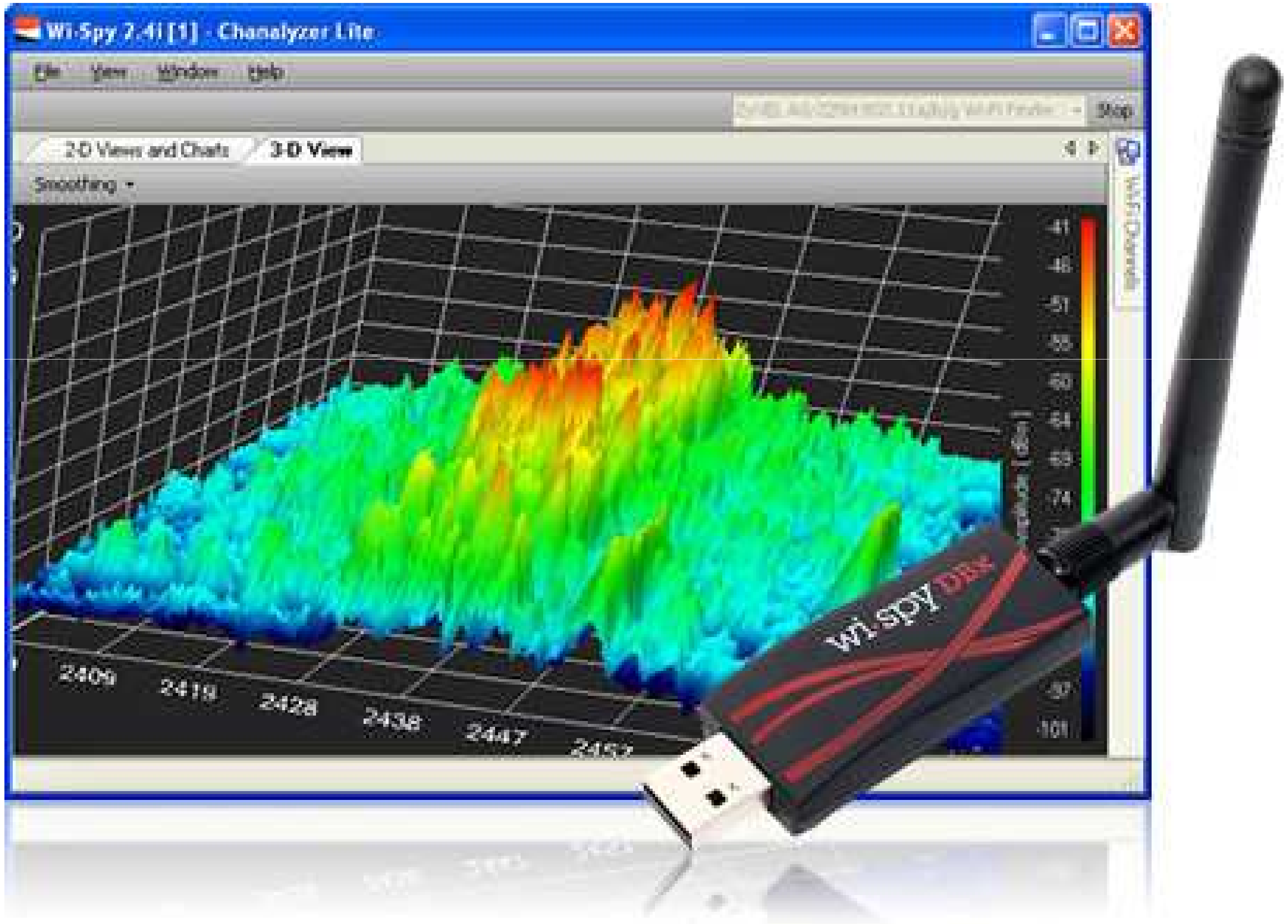
- Disponibilidad: nivel 1
  - DoS a nivel 1: Jammers o fuentes de ruido



34 APs!!!

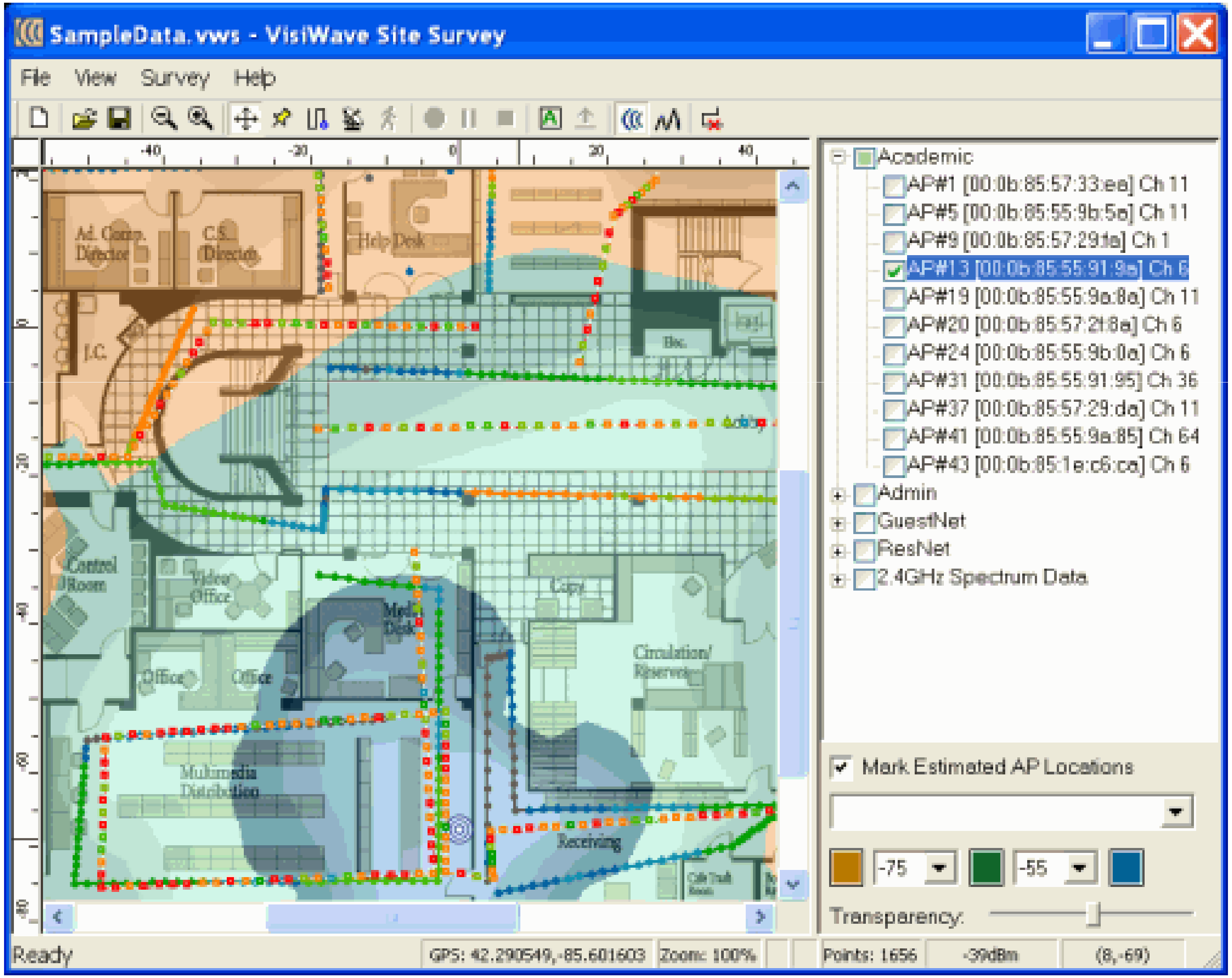
Localizar fuentes de ruido

Amenazas



Localizar fuentes de ruido

Amenazas



- ⊟ ▣ Academic
  - □ AP#1 [00:0b:85:57:33:ee] Ch 11
  - □ AP#5 [00:0b:85:55:9b:5e] Ch 11
  - □ AP#9 [00:0b:85:57:29:fa] Ch 1
  - ☑ AP#13 [00:0b:85:55:91:9a] Ch 6
  - □ AP#19 [00:0b:85:55:9a:8a] Ch 11
  - □ AP#20 [00:0b:85:57:21:8a] Ch 6
  - □ AP#24 [00:0b:85:55:9b:0a] Ch 6
  - □ AP#31 [00:0b:85:55:91:95] Ch 36
  - □ AP#37 [00:0b:85:57:29:da] Ch 11
  - □ AP#41 [00:0b:85:55:9a:85] Ch 64
  - □ AP#43 [00:0b:85:1e:c6:ca] Ch 6
- ⊞ □ Admin
- ⊞ □ GuestNet
- ⊞ □ ResNet
- ⊞ □ 2.4GHz Spectrum Data

☑ Mark Estimated AP Locations

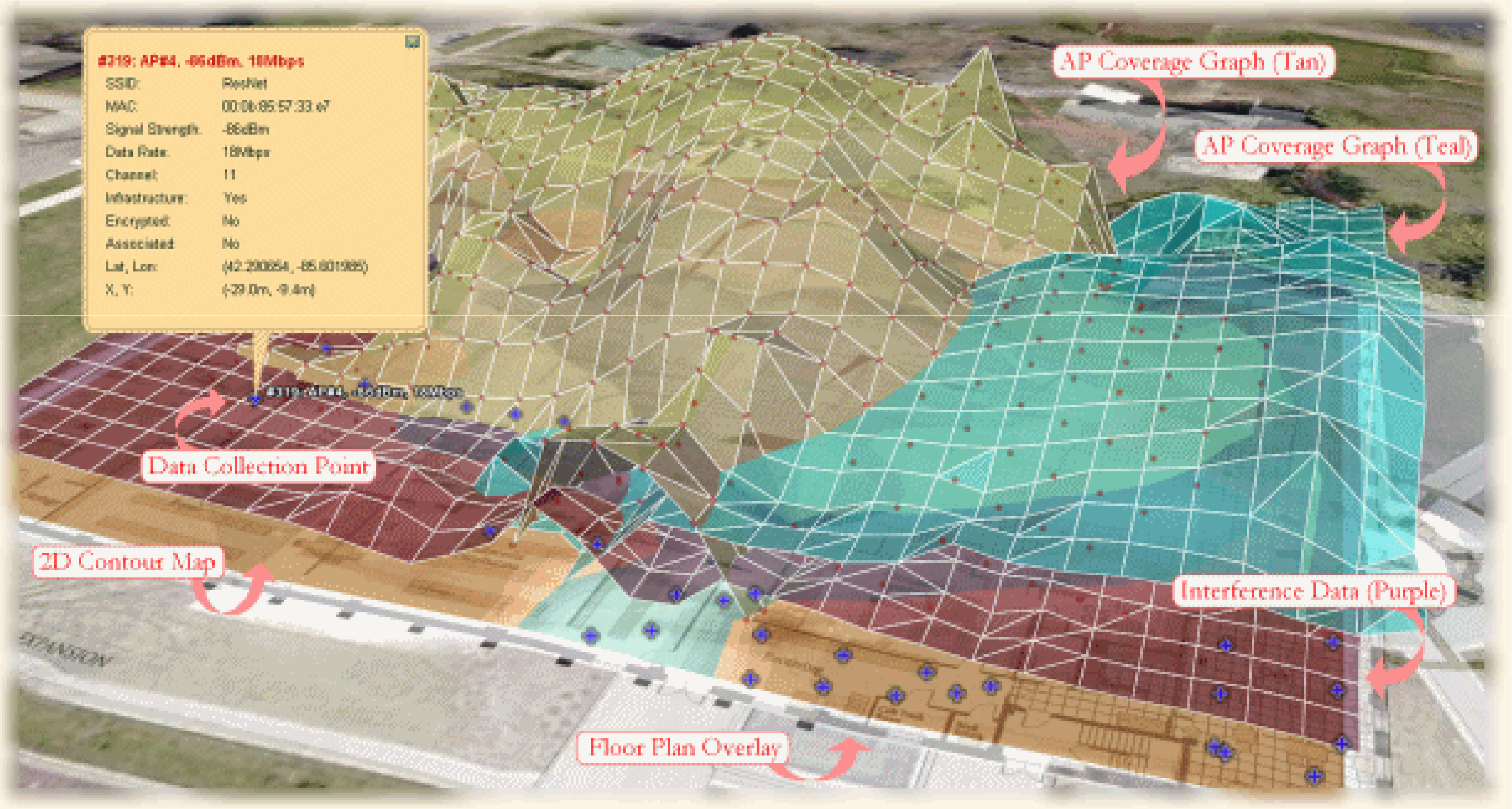
🟧 -75 🟩 -55 🟦

Transparency:

Ready | GPS: 42.290549,-85.601603 | Zoom: 100% | Points: 1656 | -39dBm | (8,-69)

Localizar fuentes de ruido

Amenazas



#319: AP#4, -86dBm, 18Mbps

SSID: RexNet

MAC: 00:0b:85:57:33:e7

Signal Strength: -86dBm

Data Rate: 18Mbps

Channel: 11

Infrastructure: Yes

Encrypted: No

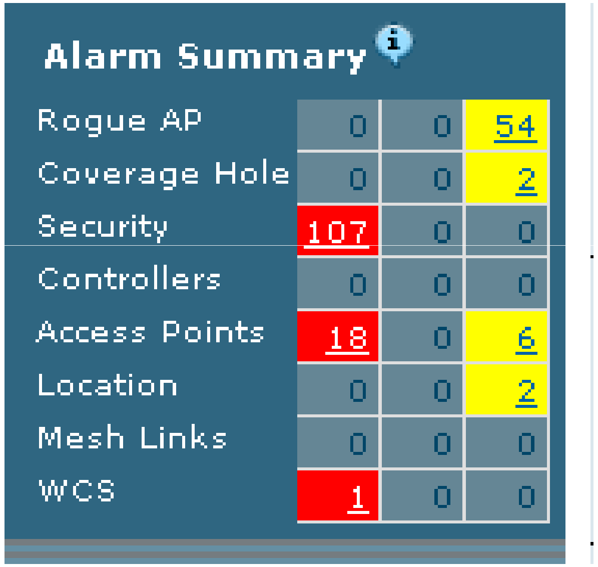
Associated: No

Lat, Lon: (42.290854, -85.601985)

X, Y: (-29.0m, -9.4m)

Consultar/correlar Logs

- Si estamos aburridos: podemos mirar logs (IDS)
  - Deautenticaciones
  - Inyecciones de tráfico
  - NetStumblers, etc…



Alarm Summary

Rogue AP	0	0	54
Coverage Hole	0	0	2
Security	107	0	0
Controllers	0	0	0
Access Points	18	0	6
Location	0	0	2
Mesh Links	0	0	0
WCS	1	0	0

- IPS-wifi ¿Activamos la protección activa?

Seamos realistas

Conclusión

- Todo este trabajo…
  - Para virtualizar un cable!!
- Hay frentes más vulnerables y fructíferos
  - “Puertas blindadas en paredes de pladur”
- Ojalá la LAN tuviera esta gestión de acceso
  - Exportar la experiencia 802.1x a la LAN

Toni Pérez Sánchez
toni.perez (at) uib.es

Universitat de les Illes Balears
Centre de Tecnologies de la Informació