

MONTAJE Y CONTROL DE UNA RED WI-FI® ASEGURADA A NIVEL EMPRESARIAL CON WPA2-ENTERPRISE

Ing. Luis Felipe Domínguez Vega

luis.dominguez@mtz.desoft.cu

H3R3T1C



Mecanismos de seguridad en Wi-Fi



Filtrado por MAC



WEP



WPA

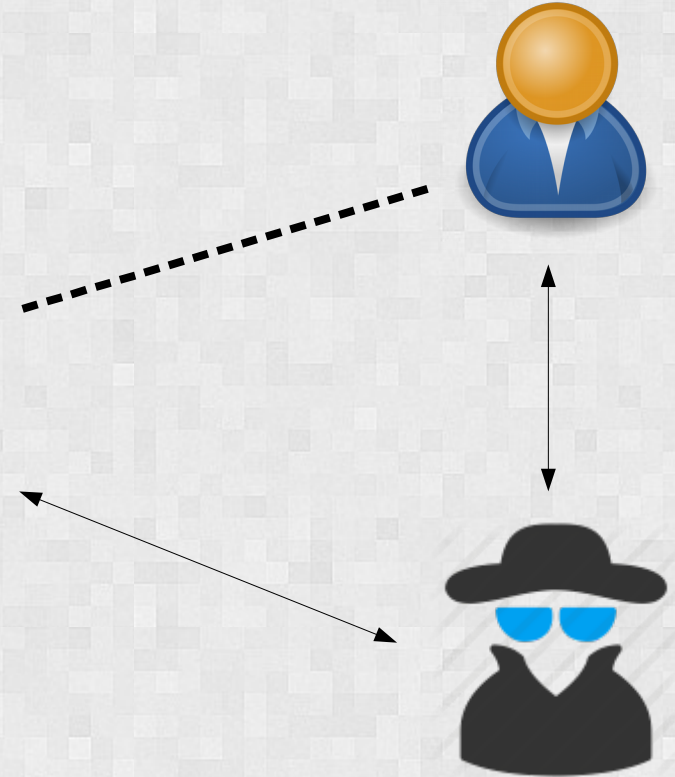
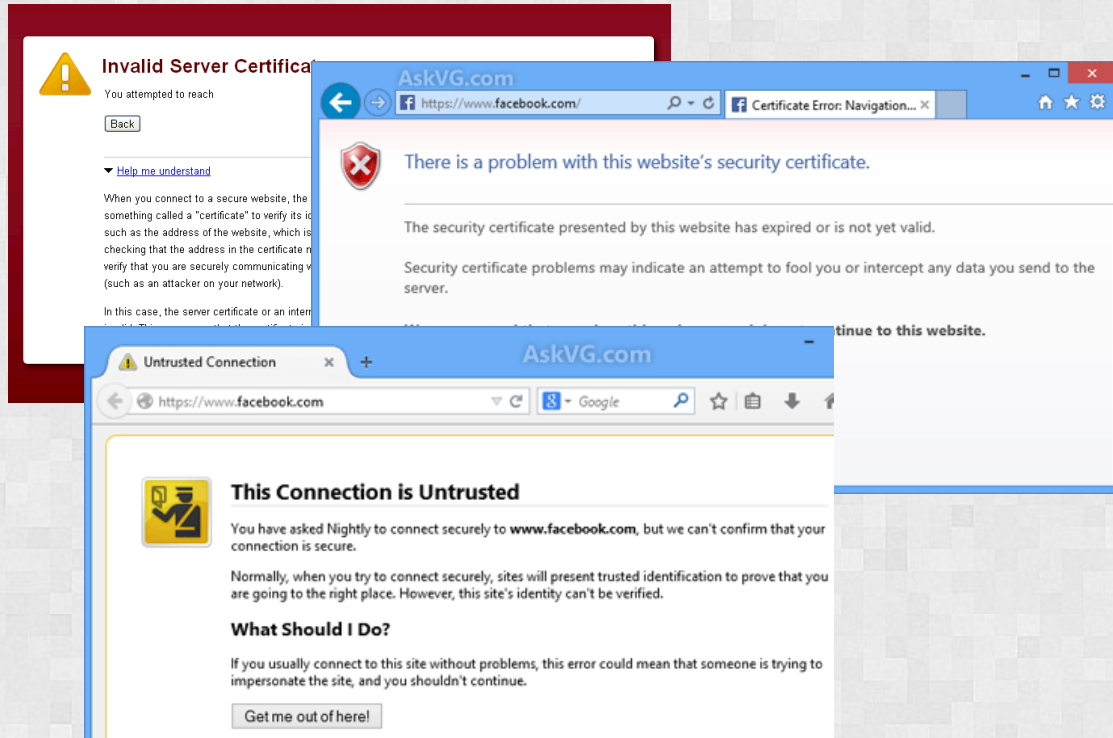


WPA2 / WPS

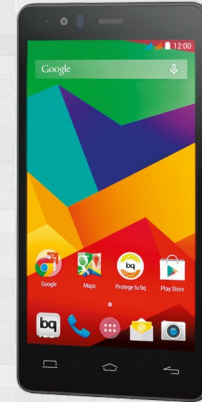
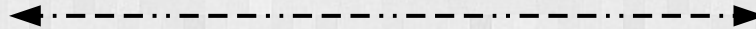


WPA2-Enterprise

SEGURIDAD CON CERTIFICADOS



EL (IN)SEGURO WPS





Poniendo en marcha el sistema

Bases

Software

- **GNU/Linux** Debian Testing 64 bits
- **Samba** 4.5.2
- **Bind9** 9.10.3
- **Freeradius** 3.0.12
- **ETK** 5.1.2
- **Grafana** 4.1.0

Hardware

Router inalámbrico TP-Link N600

Controlador Intel Core i7-4770 @
3.40 Ghz + 4 Gb

RADIUS virtualizado con 2 núcleos
de Intel Core i5-4460 @ 3.20 Ghz
+ 512 Mb RAM



Se configura el servidor de dominio Samba



Configurando el servidor de dominio Samba

1.Instalamos el paquete `samba`

2.Utilizamos `samba-tool domain provision`

3.Adicionas el grupo WiFi:

```
samba-tool group add WiFi
```

4.Adicionamos los usuarios al grupo WiFi:

```
samba-tool group addmembers WiFi usuario
```




Uniendo de manera ligera al dominio



Uniendo de manera ligera al dominio

1. Instalamos el paquete `samba` y `winbind`
2. Se modifica `/etc/samba/smb.conf`
3. Se modifica `/etc/krb5.conf`
4. Se ejecuta `net ads join`



Configurando el servidor RADIUS



Configurando el servidor RADIUS

1. Instalamos el paquete `freeradius`
2. Se modifica `/etc/freeradius/3.0/clients.conf`
3. Se modifica `/etc/freeradius/3.0/sites-enabled/default`
4. Se modifica `/etc/freeradius/3.0/mods-available/eap`



Sobre OpenWRT



Protegiendo los AP



Protegiendo los AP

AP_DESARROLLO

Authorization Required

Please enter your username and password.

Invalid username and/or password! Please try again.

Username

root

Password



Login



Reset

Powered by [LuCI 15.05-149-g0d8bbd2](#) Release ([git-15.363.78009-956be55](#)) / Open



Protegiendo los AP

AP_DESARROLLO

Status ▾System ▾Network ▾Logout

AUTO REFRESH ON

Status

System

Hostname	AP_0
Model	TP-L
Firmware Version	OpenWrt 19.07.0 / LuCI 15.05-149-g0d8bbd2 Release (git-15.363.78009-956b)
Kernel Version	3.18.23
Local Time	Thu Jan 19 16:25:19 2017
Uptime	3d 22h 43m 11s
Load Average	0.08, 0.03, 0.05

Memory

Total Available	102212 kB / 126044 kB (81%)
-----------------	-----------------------------

Interfaces

Wifi

Switch

DHCP and DNS

Hostnames

Static Routes

Firewall

Diagnostics



Protegiendo los AP

AP_DESARROLLO

Status ▾

System ▾

Network ▾

Logout

AUTO REFRESH ON

Wireless Overview



Generic MAC80211 802.11bgn (radio0)

Channel: 7 (2.442 GHz) | Bitrate: ? Mbit/s



Scan



Add



SSID: [REDACTED]

Mode: Master

0%

BSSID: [REDACTED]

Encryption: WPA2 802.1X (CCMP)



Disable



Edit



Remove

Edit this network



Atheros AR9580 802.11an (radio1)

Channel: 128 (5.640 GHz) | Bitrate: ? Mbit/s



Scan



Add



SSID: [REDACTED]

Mode: Master

0%

BSSID: [REDACTED]

Encryption: WPA2 802.1X (CCMP)



Disable



Edit



Remove

Associated Stations

SSID

MAC-Address

IPv4-Address

Signal

Noise

RX Rate

TX Rate

No information available



Protegiendo los AP

AP_DESARROLLO

Status ▾System ▾Network ▾Logout

AUTO REFRESH ON

Interface Configuration

General Setup

Wireless Security

MAC-Filter

ESSID

Mode

Access Point (WDS) ▾

Network

☐

lan:

☒wan:

☐create:

Hide ESSID

☐

WMM Mode

☒



Protegiendo los AP

AP_DESARROLLO Status ▾ System ▾ Network ▾ Logout

Interface Configuration

General Setup Wireless Security MAC-Filter

Encryption WPA2-EAP ▾

Cipher Force CCMP (AES) ▾

Radius-Authentication-Server

Radius-Authentication-Port
Default 1812

Radius-Authentication-Secret

Radius-Accounting-Server

Radius-Accounting-Port
Default 1813

Radius-Accounting-Secret

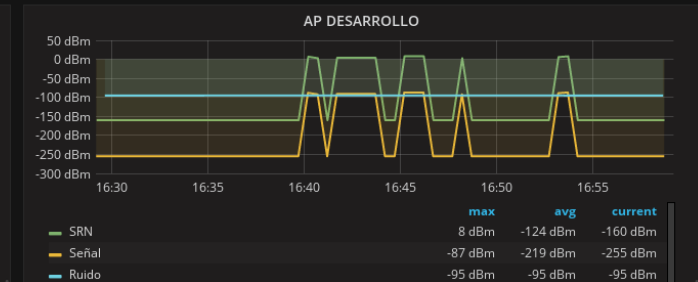
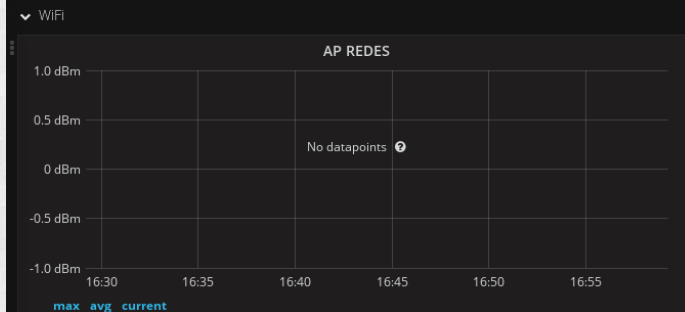
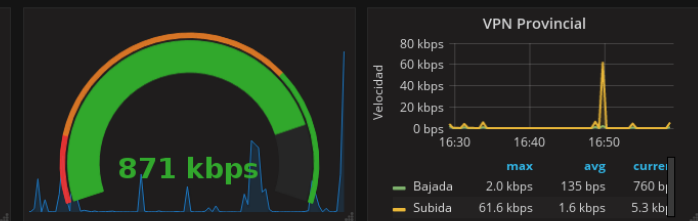
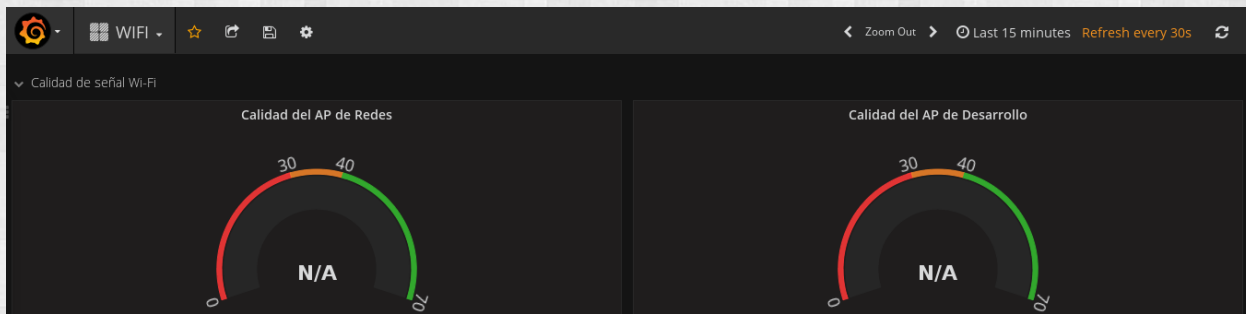
NAS ID DESARROLLO 2.4Ghz



ETK + Grafana



ETK + Grafana



CONCLUSIONES

MONTAJE Y CONTROL DE UNA RED WI-FI® ASEGURADA A NIVEL EMPRESARIAL CON WPA2-ENTERPRISE

Ing. Luis Felipe Domínguez Vega

luis.dominguez@mtz.desoft.cu

H3R3T1C