Universitat Oberta de Catalunya

Diseño e implementación de redes Wi-Fi seguras

Autor: Rafael César Baldeón Guillama

Tutora: María Isabel March Hermo

Trabajo Fin de Grado (06/2019)

Área: Redes de Computadores

Índice

1. Introducción
2. Redes inalámbricas (Wi-Fi)
3. Seguridad en redes Wi-Fi
4. Medidas adicionales
5. Perfiles de seguridad
6. Recomendaciones generales
7. Casos prácticos
8. Conclusiones

Introducción

- Incremento de redes Wi-Fi en todos los entornos
  - Fácil instalación, flexibilidad y bajo coste
- Peligros de las redes Wi-Fi
  - Dispositivos no actualizados (*firmware)* y vulnerabilidades sin parchear
  - Uso en sitios públicos de Redes abiertas
  - Utilización de protocolos de seguridad vulnerables
- Amenazas en Internet
  - Aumento de ataques sobre Internet (email, webs, etc.)
  - Equipos poco protegidos (aplicaciones de seguridad en el ordenador)

Redes inalámbricas (Wi-Fi)

- Interconexión a través de ondas electromagnéticas (sin cables)
- Organización Wi-Fi Alliance
  - Marca comercial Wi-Fi (Wireless Fidelity) año 1997
  - Certificar productos sobre el estándar 802.11

Logotipo certificado Wi-Fi

Seguridad en redes Wi-Fi

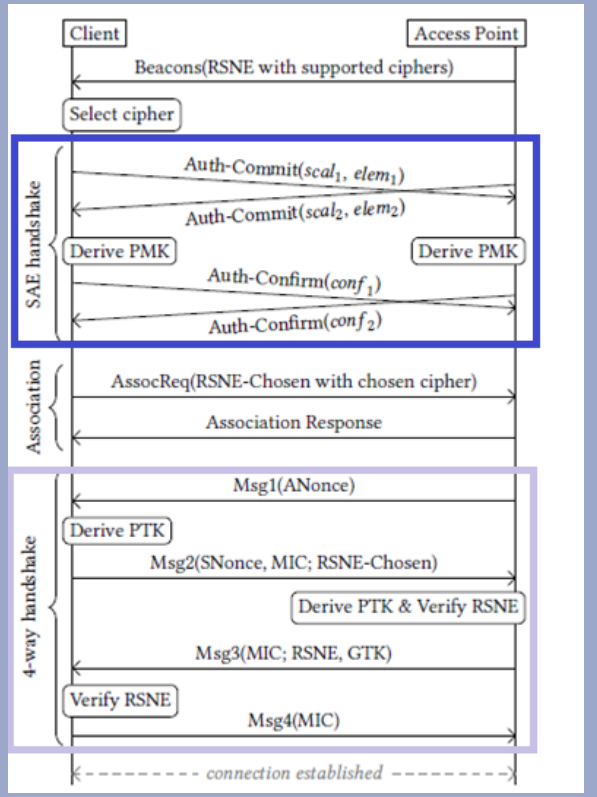
- **Protocolos de seguridad actuales**
  - ✖ WEP (Año 1997) Vulnerable
  - ✖ WPA/WPA2 (Año 2004/2007) Vulnerable
  - ✖ WPS (Año 2007) Vulnerable

Seguridad en redes Wi-Fi

- **Nuevas certificaciones de seguridad (Wi-Fi Alliance)**
  - WPA3 (Personal y Enterprise)
  - Wi-Fi Enhanced Open
  - Wi-Fi Easy Connect

Seguridad en redes Wi-Fi

- **WPA3-Personal**
  - Sistema SAE (*Simultaneous Authentication of Equals*)
  - Aporta las características de seguridad:
    - ✓ PFS (*Perfect Forward Secrecy*)
    - ✓ Protección a los ataques de diccionario
  - PMF (*Protection Management Frame*) obligatorio



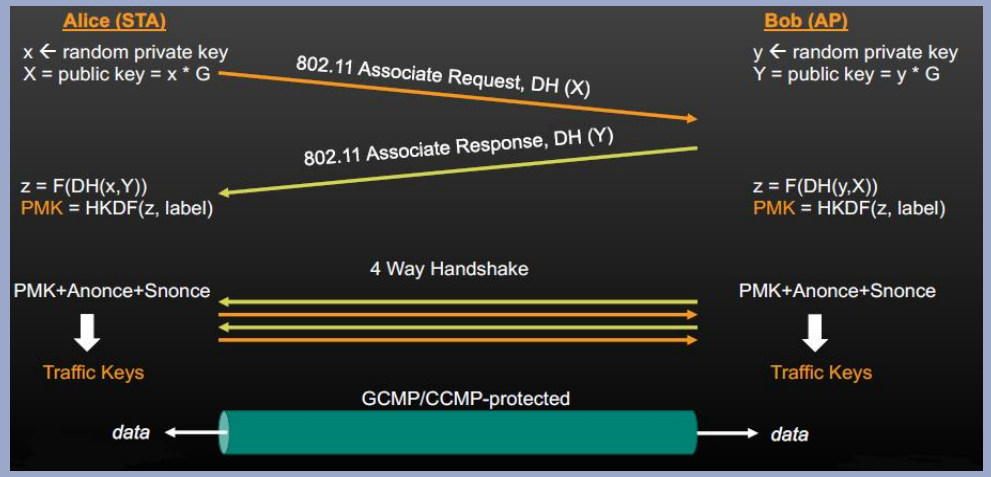
Handshake WPA3-Personal

Seguridad en redes Wi-Fi

- **WPA3-Enterprise**
  - Herramientas criptográfica mejoradas
  - Clave 192 bits (Opcional)
  - PMF Robusto (256 bits)

Seguridad en redes Wi-Fi

- **Wi-Fi Enhanced Open**
  - Desarrollado para sustituir las implementaciones de redes abiertas
  - Envío y recepción de información cifrada
  - Protocolo OWE (*Opportunistic Wireless Encryption)*
    - ✓ Protocolo *Diffie-Hellman* (Intercambio de clave)



Handshake OWE

Seguridad en redes Wi-Fi

- **Wi-Fi Easy Connect**
  - Reemplazar protocolo WPS
  - Configurador (Lectura de código QR y envío configuración)
  - Cifrado robusto (Clave pública)

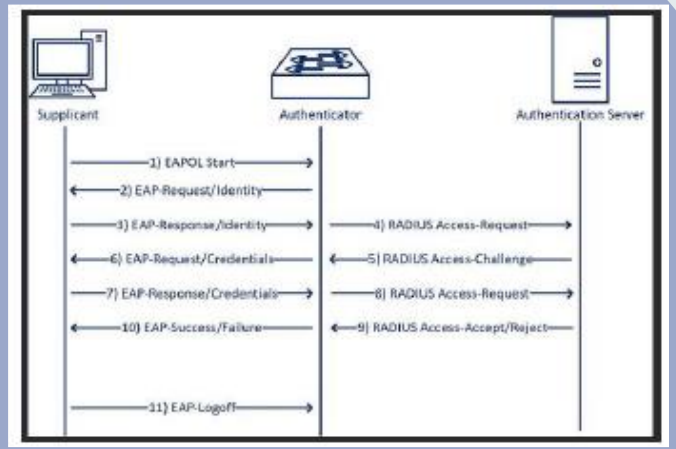
Proceso conexión dispositivos con Easy Connect

Medidas adicionales

- **Protocolo 802.1X**

Control a nivel de puerto mediante autentificación.

  - Métodos:
    - ✓ PEAP: Certificado en el servidor
    - ✓ EAP-TLS: Certificado en cliente y servidor
    - ✓ EAP-TTLS: Certificado en servidor



Conexión EAP Radius

- **NAC (Network Access Control)**

Control de los dispositivos que se conectan a la infraestructura de red.

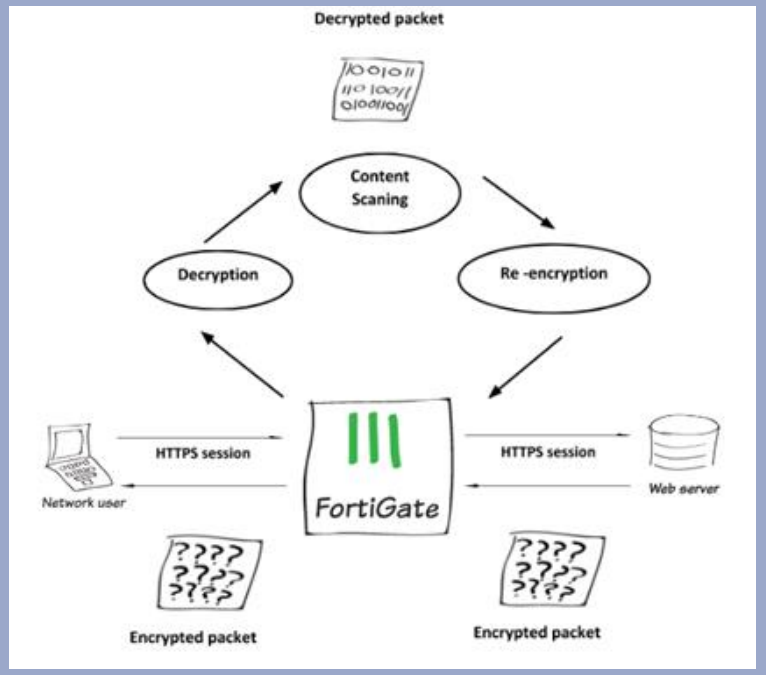
- **WIDS/WIPS**

WIDS: Sistema para detectar e informar intrusiones en las redes Wi-Fi

WIPS: Sistema para detectar intrusiones en las redes Wi-Fi, y ejecutar una contramedida.

Perfiles de seguridad

- Sistemas que actúan como medidas de defensa
  - Firewall
  - IDS/IPS
  - Antimalware
  - Application Control
  - Web Filtering
  - Data Loss Prevention
  - SSL-Inspection



SSL-Inspection

- Conjuntamente forman un perfil de seguridad

Recomendaciones generales

- **Dispositivos de interconexión**
  - ✓ Adquisición de equipos certificados (Wi-Fi Alliance)
  - ✓ Protocolo conexión seguros para la gestión dispositivos (HTTPS/SSH)
  - ✓ Modificar claves de acceso a los dispositivos
  - ✓ Actualización *firmware* y aplicar parches de seguridad
  - ✓ Mínima funcionalidad
  - ✓ Definir franjas horarias de uso de la red

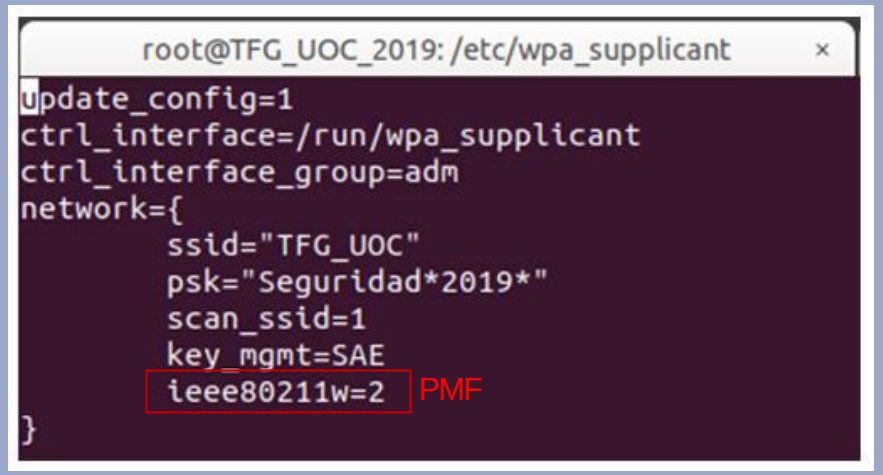
Casos prácticos

- Entornos más comunes
  - Doméstico
  - Sitios públicos
  - Corporativos
- Firewall UTM (Perfiles de seguridad)

Casos prácticos

- **Doméstico**
  - Configuración de WPA3-Personal

Configuración Router



Configuración Cliente

Casos prácticos

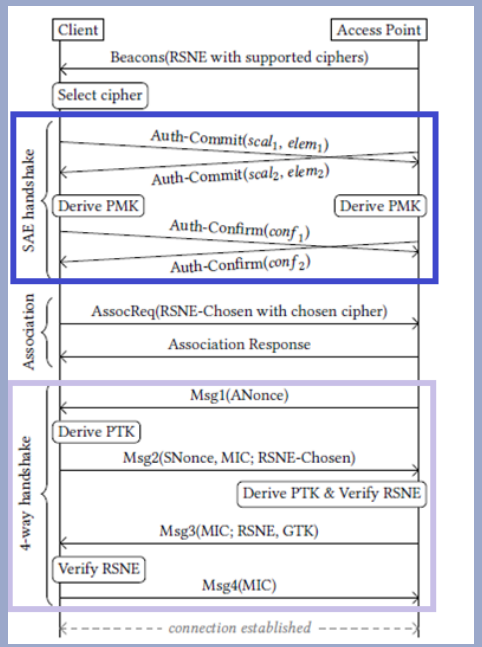
- **Doméstico**
  - Verificar la aplicación del sistema SAE para mejorar la seguridad en el proceso de autenticación.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Synology_a4:e7:57	Broadcast	802.11	306	Beacon frame, SN=338, FN=0, Flags=........, BI=100, SSID=Wildcard (Broadcast)
2	4.610818	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	307	Probe Response, SN=212, FN=0, Flags=........, BI=100, SSID=TFG_UOC
3	4.610828		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
4	9.203276	LiteonTe_e1:6e:1b	Synology_a4:e7:57	802.11	128	Authentication, SN=257, FN=0, Flags=........
5	9.203780		LiteonTe_e1:6e:1b (…	802.11	10	Acknowledgement, Flags=........
6	9.362498	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	128	Authentication, SN=213, FN=0, Flags=........
7	9.363018		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
8	9.395274	LiteonTe_e1:6e:1b	Synology_a4:e7:57	802.11	64	Authentication, SN=258, FN=0, Flags=........
9	9.395780		LiteonTe_e1:6e:1b (…	802.11	10	Acknowledgement, Flags=........
10	9.397826	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	64	Authentication, SN=214, FN=0, Flags=........
11	9.397834		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
12	9.405514	LiteonTe_e1:6e:1b	Synology_a4:e7:57	802.11	161	Association Request, SN=259, FN=0, Flags=........, SSID=TFG_UOC
13	9.405508		LiteonTe_e1:6e:1b (…	802.11	10	Acknowledgement, Flags=........
14	9.410114	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	200	Association Response, SN=215, FN=0, Flags=........
15	9.410124		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
16	9.433154	Synology_a4:e7:57	LiteonTe_e1:6e:1b	EAPOL	155	Key (Message 1 of 4)
17	9.433164		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
18	9.435724	LiteonTe_e1:6e:1b	Synology_a4:e7:57	EAPOL	161	Key (Message 2 of 4)
19	9.436226		LiteonTe_e1:6e:1b (…	802.11	10	Acknowledgement, Flags=........
20	9.449026	Synology_a4:e7:57	LiteonTe_e1:6e:1b	EAPOL	221	Key (Message 3 of 4)
21	9.449034		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
22	9.452108	LiteonTe_e1:6e:1b	Synology_a4:e7:57	EAPOL	133	Key (Message 4 of 4)
23	9.452100		LiteonTe_e1:6e:1b (…	802.11	10	Acknowledgement, Flags=........

SAE-Handshake

Asociación

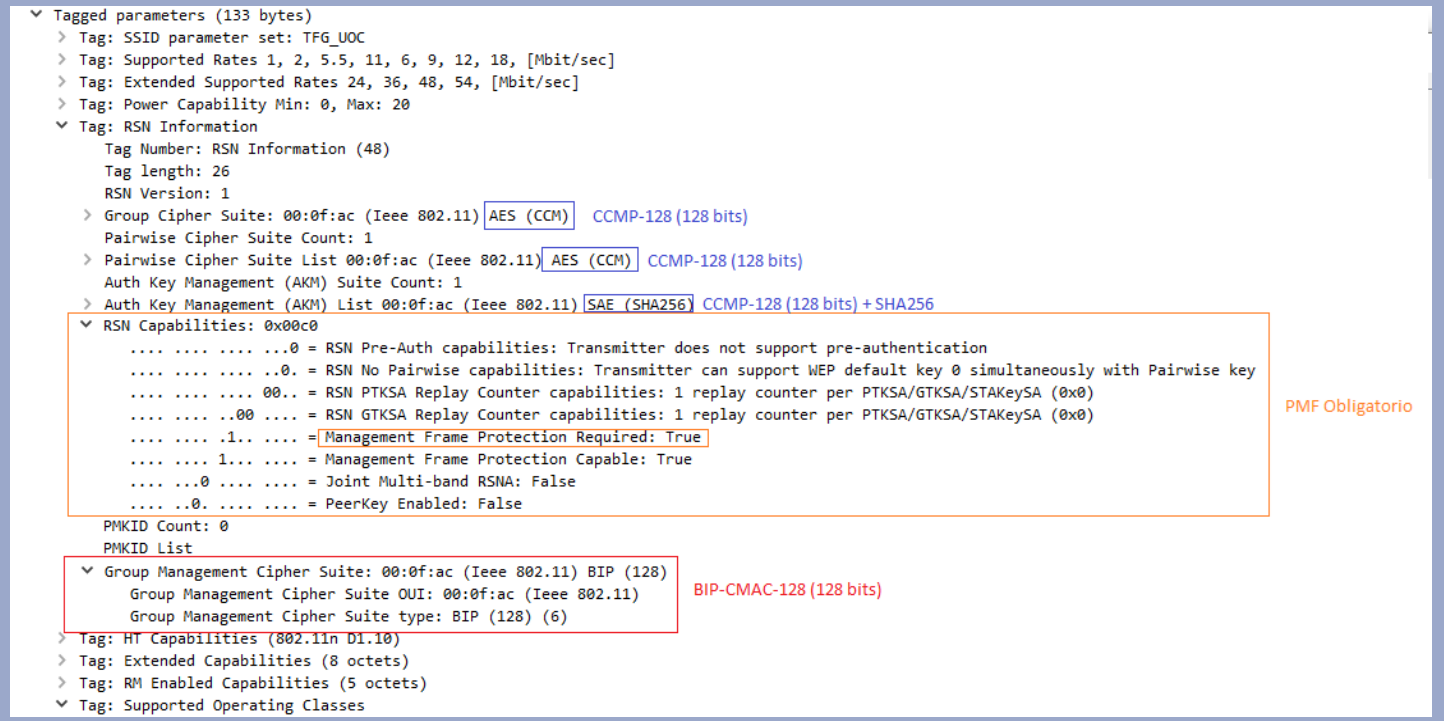
4-way Handshake



Handshake SAE

Casos prácticos

- **Doméstico**
  - Aplicación de PMF para proteger las tramas de control y gestión.



PMF obligatorio

Casos prácticos

- **Sitios públicos**
  - Configuración de Wi-Fi Enhanced Open (OWE).

Configuración Router

```
update_config=1
ctrl_interface=/run/wpa_supplicant
ctrl_interface_group=adm
network={
        ssid="TFG_UOC_INVITADOS"
        ieee80211w=2
        key_mgmt=OWE
}
```

PMF

Configuración Cliente

Casos prácticos

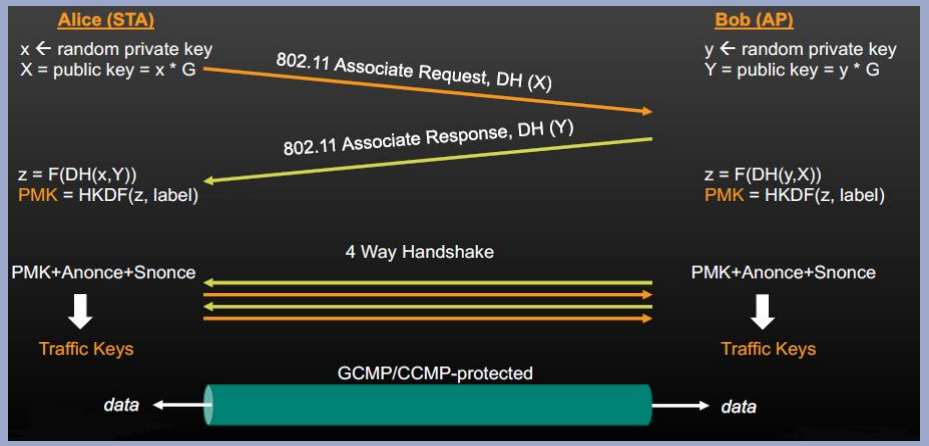
- **Sitios públicos**
  - Verificar la aplicación del protocolo OWE.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Synology_a4:e7:57	Broadcast	802.11	323	Beacon frame, SN=352, FN=0, Flags=........, BI=100, SSID=TFG_UOC_INVITADOS
2	4.074750	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	317	Probe Response, SN=218, FN=0, Flags=........, BI=100, SSID=TFG_UOC_INVITADOS
3	4.074760		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
4	8.663110	LiteonTe_e1:6e:1b	Synology_a4:e7:57	802.11	30	Authentication, SN=257, FN=0, Flags=........
5	8.663614		LiteonTe_e1:6e:1b (…	802.11	10	Acknowledgement, Flags=........
6	8.667710	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	30	Authentication, SN=219, FN=0, Flags=........
7	8.668230		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
8	8.673350	LiteonTe_e1:6e:1b	Synology_a4:e7:57	802.11	208	Association Request, SN=258, FN=0, Flags=........, SSID=TFG_UOC_INVITADOS
9	8.673344		LiteonTe_e1:6e:1b (…	802.11	10	Acknowledgement, Flags=........
10	8.693822	Synology_a4:e7:57	LiteonTe_e1:6e:1b	802.11	259	Association Response, SN=220, FN=0, Flags=........
11	8.693832		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
12	8.716862	Synology_a4:e7:57	LiteonTe_e1:6e:1b	EAPOL	133	Key (Message 1 of 4)
13	8.716870		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
14	8.718918	LiteonTe_e1:6e:1b	Synology_a4:e7:57	EAPOL	161	Key (Message 2 of 4)
15	8.719422		LiteonTe_e1:6e:1b (…	802.11	10	Acknowledgement, Flags=........
16	8.732222	Synology_a4:e7:57	LiteonTe_e1:6e:1b	EAPOL	221	Key (Message 3 of 4)
17	8.732742		Synology_a4:e7:57 (…	802.11	10	Acknowledgement, Flags=........
18	8.734792	LiteonTe_e1:6e:1b	Synology_a4:e7:57	EAPOL	133	Key (Message 4 of 4)
19	8.735296		LiteonTe_e1:6e:1b (…	802.11	10	Acknowledgement, Flags=........

Asociación

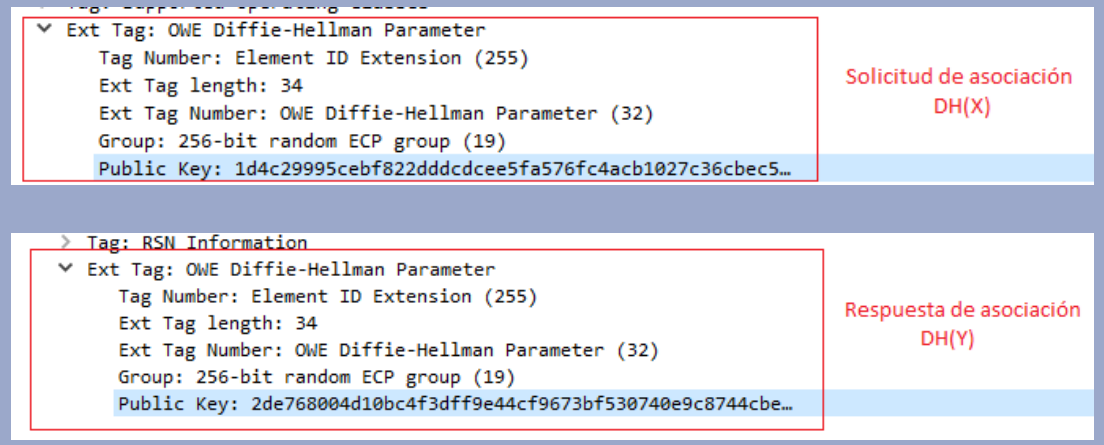
4way-Handshake

Handshake OWE



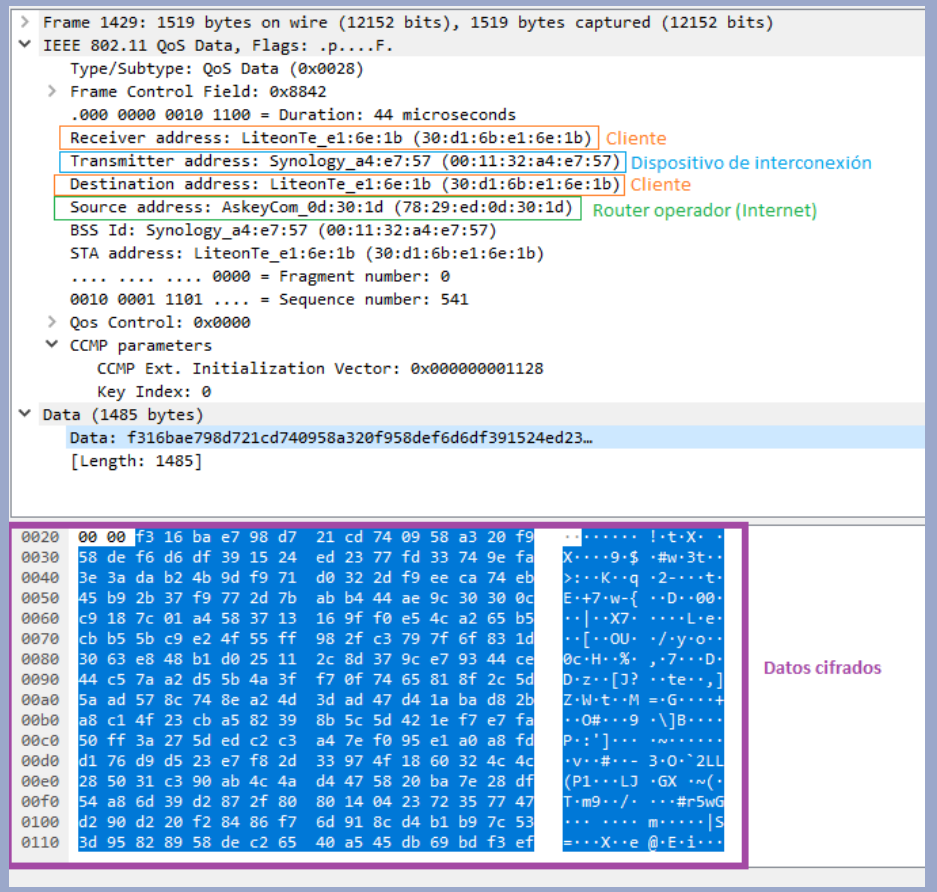
Casos prácticos

- **Sitios públicos**
  - Intercambio de claves públicas.



Protocolo Diffie-Hellman

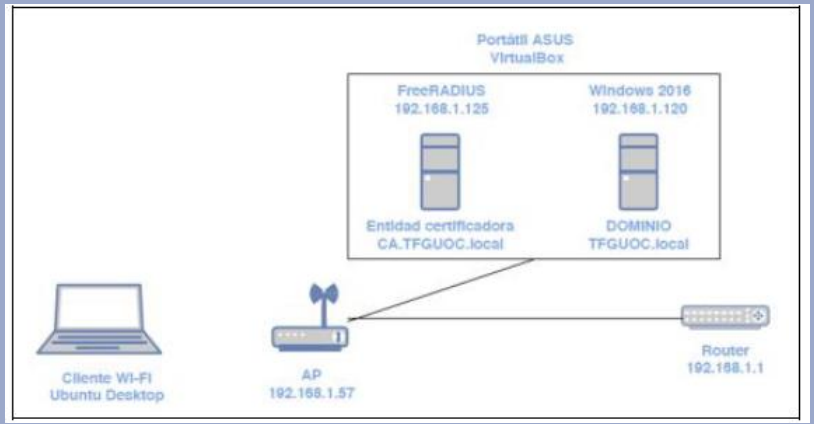
  - Envío de datos cifrados (CCMP).



Envío de datos

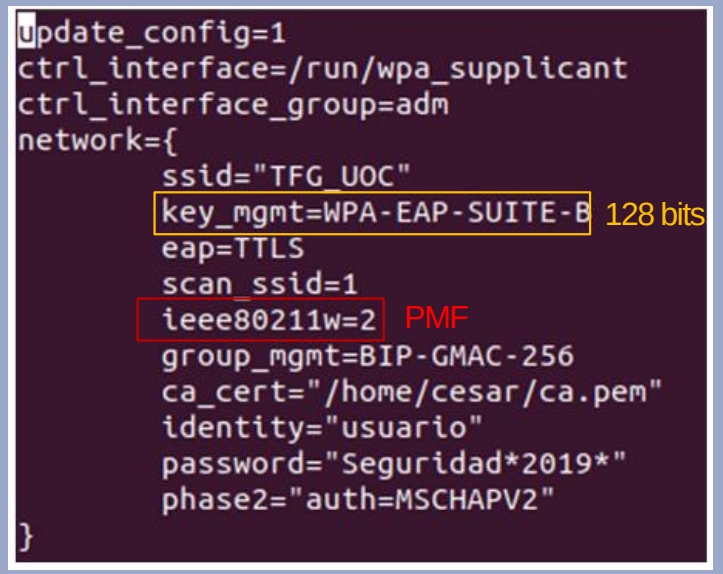
Casos prácticos

- **Corporativos**
  - Configuración de WPA3-Enterprise (128 bits)



Topología WPA3-Enterprise

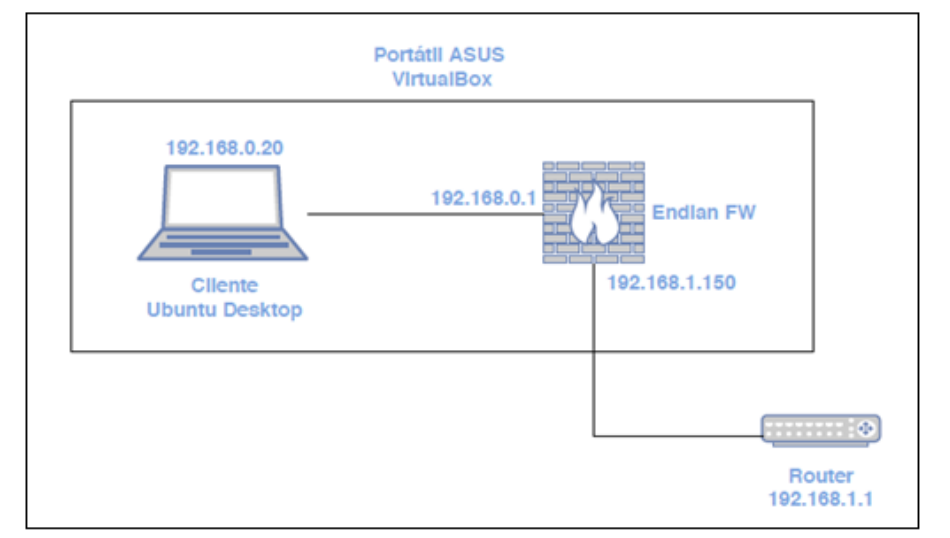
Configuración Router



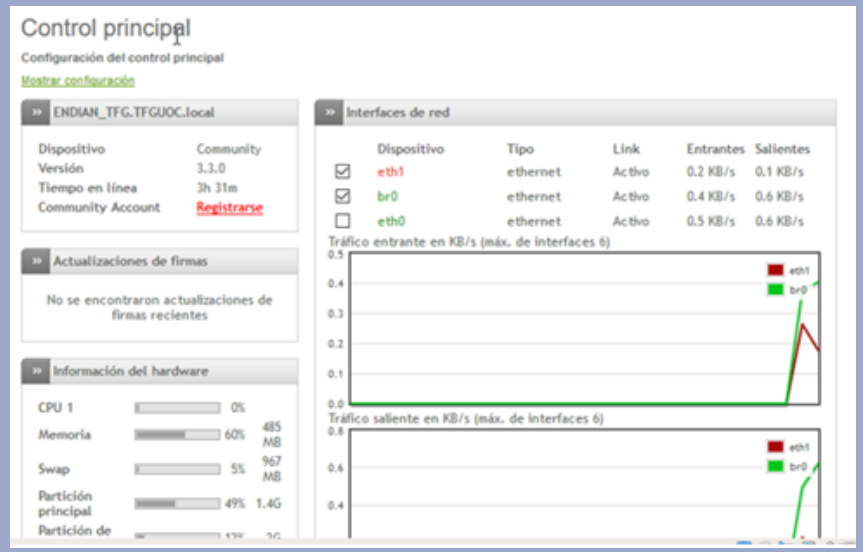
Configuración Cliente

Casos prácticos

- **Perfiles de seguridad**
  - Configuración de un Firewall UTM (Endian FW Community Edition)



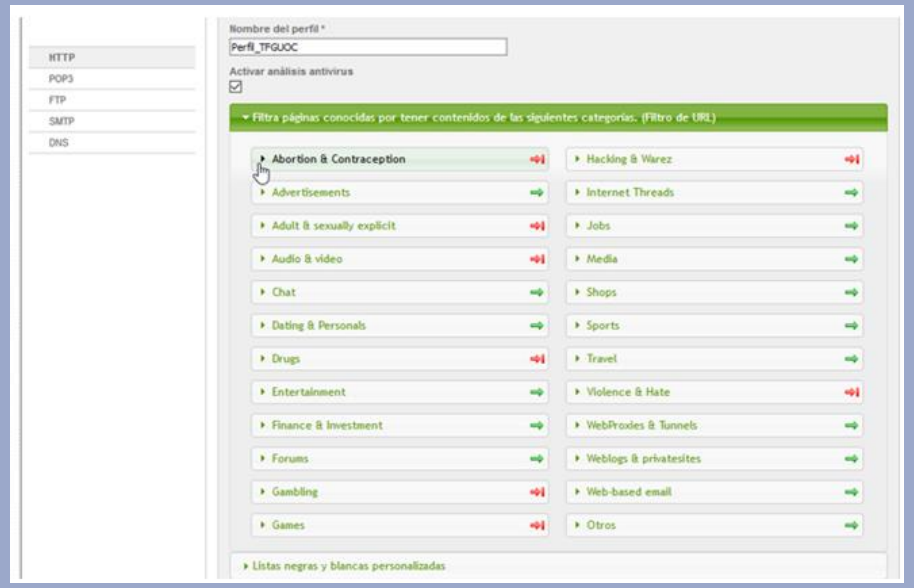
Topología FW UTM



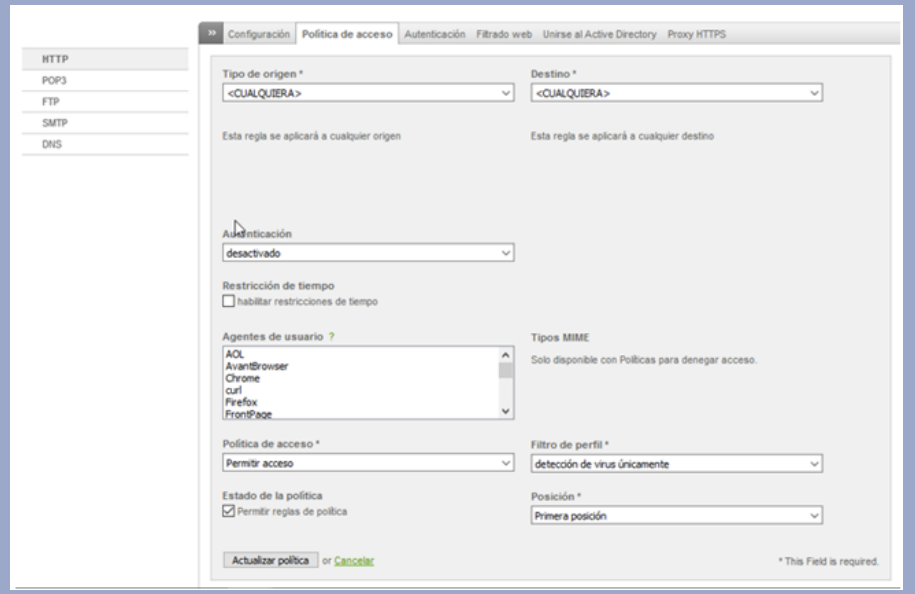
Página Principal

Casos prácticos

- **Perfiles de seguridad**
  - Configuración de WebFiltering (Control de contenidos web)
  - Configuración de Antivirus (Control de *malware*)



Web Filtering



Antivirus

Casos prácticos

- **Perfiles de seguridad**
  - Funcionamiento del sistema WebFiltering (Bloqueo contenido prohibido)
  - Funcionamiento del sistema Antivirus (Detección y bloqueo de virus)

Bloqueo del contenido no permitido

Detección de virus

Conclusiones

- Aplicar las recomendaciones generales en los dispositivos de interconexión
- Configurar los siguientes protocolos de seguridad:
  - ✗ WEP/WPA/WPA2 → ✓ WPA3
  - ✗ Redes abiertas → ✓ Wi-Fi Enhanced Open (OWE)
  - ✗ WPS → ✓ Wi-Fi Easy Connect
- En entornos corporativos, implantar NAC y sistemas WIDS/WIPS
- Monitorizar las conexiones y el tráfico que circula por la red.
- Controlar los accesos a Internet con equipos Firewall UTM (Perfiles de seguridad)

Universitat Oberta de Catalunya

Muchas gracias