

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

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

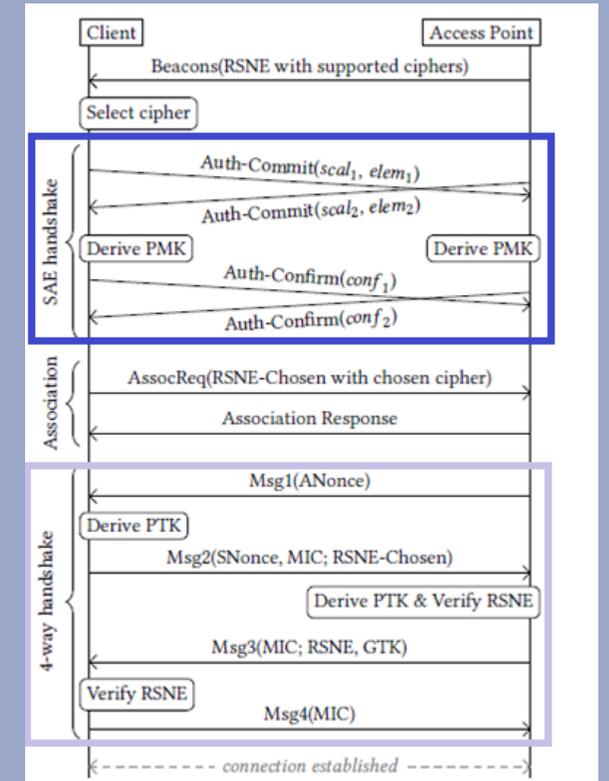


Wi-Fi CERTIFIED Easy Connect™

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



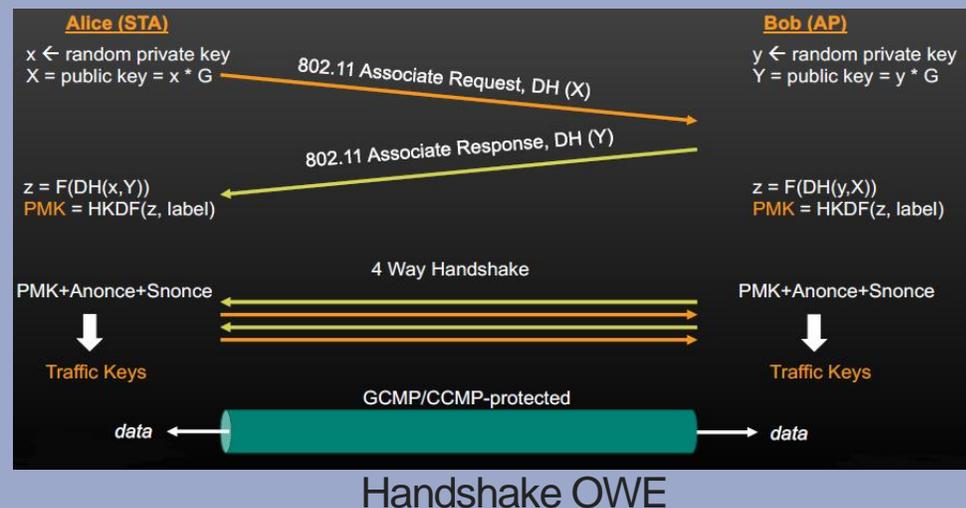
Handshake WPA3-Personal

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)



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 autenticación.

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

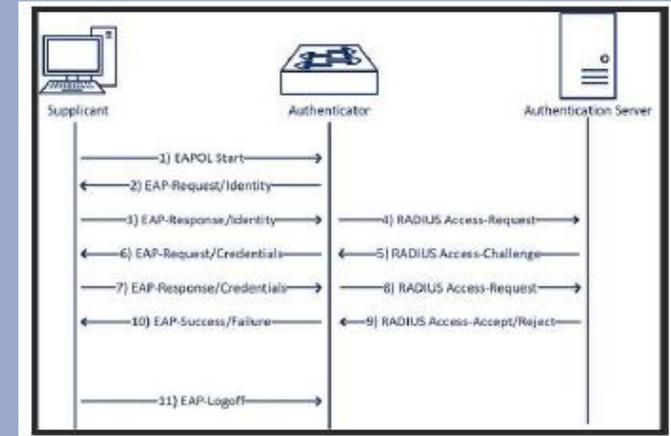
○ NAC (Network Access Control)

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

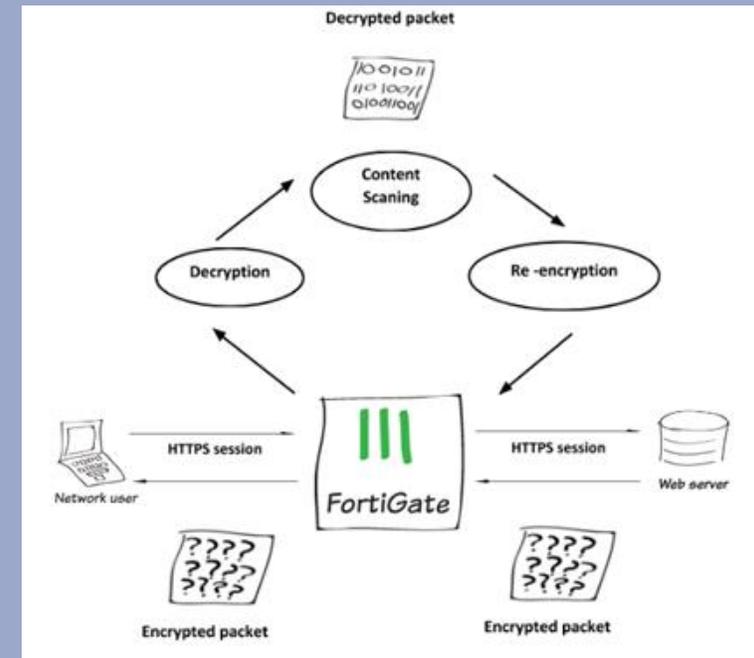
WIPS: Sistema para detectar intrusiones en las redes Wi-Fi, y ejecutar una contramedida.



Conexión EAP Radius

Perfiles de seguridad

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



SSL-Inspection

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

Nombre (SSID):	TFG_UOC	Ocultar ▼
Nivel de seguridad:	WPA3-Personal ▼	
Contraseña:	Seguridad*2019*	👁

Compatibilidad con PMF:	Activado - Obligatorio ▼
-------------------------	--------------------------

Configuración Router

```
root@TFG_UOC_2019: /etc/wpa_supplicant
update_config=1
ctrl_interface=/run/wpa_supplicant
ctrl_interface_group=adm
network={
    ssid="TFG_UOC"
    psk="Seguridad*2019*"
    scan_ssid=1
    key_mgmt=SAE
    ieee80211w=2 PMF
}
```

Configuración Cliente

Casos prácticos

○ Doméstico

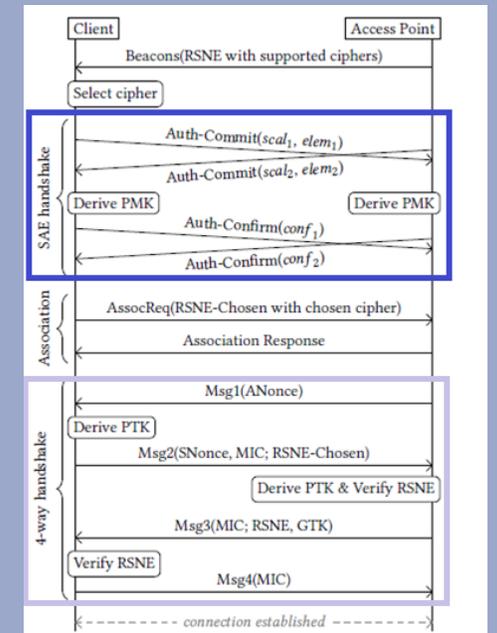
- Verificar la aplicación del sistema SAE para mejorar la seguridad en el proceso de autenticación.

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	LiteonTe_e1:6e:1b	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	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	LiteonTe_e1:6e:1b	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	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	LiteonTe_e1:6e:1b	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	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	LiteonTe_e1:6e:1b	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	LiteonTe_e1:6e:1b	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	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	LiteonTe_e1:6e:1b	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	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....

SAE-Handshake

Asociación

4-way Handshake



Casos prácticos

○ Doméstico

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

```
▼ Tagged parameters (133 bytes)
  > Tag: SSID parameter set: TFG_UOC
  > Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
  > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
  > Tag: Power Capability Min: 0, Max: 20
  ▼ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
    > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM) CCMP-128 (128 bits)
    Pairwise Cipher Suite Count: 1
    > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) CCMP-128 (128 bits)
    Auth Key Management (AKM) Suite Count: 1
    > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256) CCMP-128 (128 bits) + SHA256
    ▼ RSN Capabilities: 0x00c0
      .... = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
      .... = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STakeySA (0x0)
      .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STakeySA (0x0)
      .... = Management Frame Protection Required: True
      .... = Management Frame Protection Capable: True
      .... = Joint Multi-band RSNA: False
      .... = PeerKey Enabled: False
    PMKID Count: 0
    PMKID List
    ▼ Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
      Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Group Management Cipher Suite type: BIP (128) (6)
  > Tag: HT Capabilities (802.11n D1.10)
  > Tag: Extended Capabilities (8 octets)
  > Tag: RM Enabled Capabilities (5 octets)
  ▼ Tag: Supported Operating Classes
```

PMF Obligatorio

BIP-CMAC-128 (128 bits)

PMF obligatorio

Casos prácticos

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

Nombre (SSID):	TFG_UOC_INVITADOS
Nivel de seguridad:	OWE
Conexiones máx.:	128

Configuración Router

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

Configuración Cliente

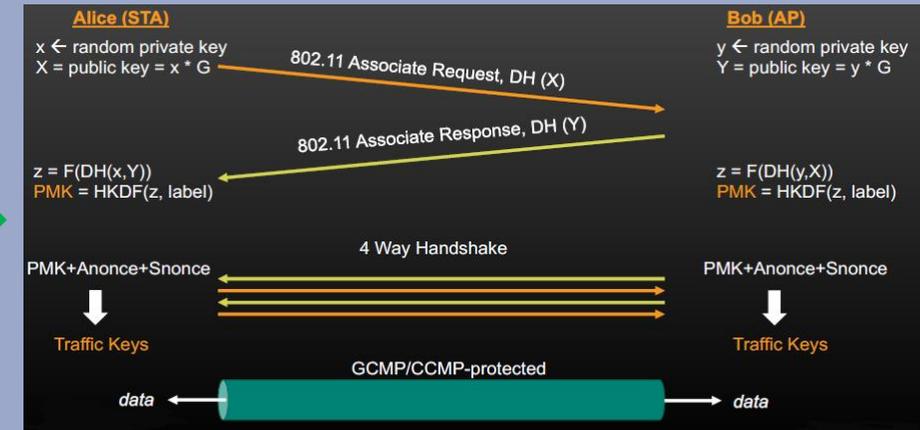
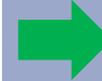
Casos prácticos

- 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	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	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	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	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	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	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	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	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	LiteonTe_e1:6e:1b	802.11	10	Acknowledgement, Flags=.....

Asociación

4way-Handshake



Handshake OWE

Casos prácticos

○ Sitios públicos

■ Intercambio de claves públicas.

```

  > Ext Tag: OWE Diffie-Hellman Parameter
    Tag Number: Element ID Extension (255)
    Ext Tag length: 34
    Ext Tag Number: OWE Diffie-Hellman Parameter (32)
    Group: 256-bit random ECP group (19)
    Public Key: 1d4c29995cebf822ddcdcee5fa576fc4acb1027c36cbec5...
  
```

Solicitud de asociación
DH(X)

```

  > Tag: RSN Information
  > Ext Tag: OWE Diffie-Hellman Parameter
    Tag Number: Element ID Extension (255)
    Ext Tag length: 34
    Ext Tag Number: OWE Diffie-Hellman Parameter (32)
    Group: 256-bit random ECP group (19)
    Public Key: 2de768004d10bc4f3dff9e44cf9673bf530740e9c8744cbe...
  
```

Respuesta de asociación
DH(Y)

Protocolo Diffie-Hellman

■ Envío de datos cifrados (CCMP).

```

  > Frame 1429: 1519 bytes on wire (12152 bits), 1519 bytes captured (12152 bits)
  > IEEE 802.11 QoS Data, Flags: .p....F.
    Type/Subtype: QoS Data (0x0028)
    > Frame Control Field: 0x8842
      .000 0000 0010 1100 = Duration: 44 microseconds
      Receiver address: LiteonTe_e1:6e:1b (30:d1:6b:e1:6e:1b) Cliente
      Transmitter address: Synology_a4:e7:57 (00:11:32:a4:e7:57) Dispositivo de interconexión
      Destination address: LiteonTe_e1:6e:1b (30:d1:6b:e1:6e:1b) Cliente
      Source address: AskeyCom_0d:30:1d (78:29:ed:0d:30:1d) Router operador (Internet)
      BSS Id: Synology_a4:e7:57 (00:11:32:a4:e7:57)
      STA address: LiteonTe_e1:6e:1b (30:d1:6b:e1:6e:1b)
      .... = Fragment number: 0
      0010 0001 1101 .... = Sequence number: 541
    > Qos Control: 0x0000
    > CCMP parameters
      CCMP Ext. Initialization Vector: 0x000000001128
      Key Index: 0
    > Data (1485 bytes)
      Data: f316bae798d721cd740958a320f958def6d6df391524ed23...
      [Length: 1485]
  
```

```

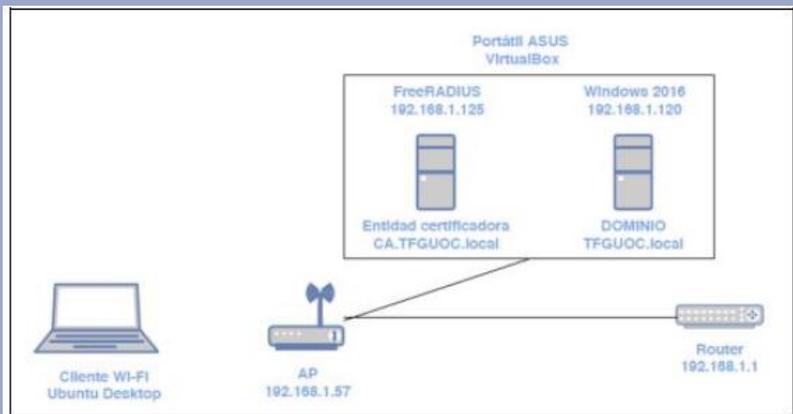
  0020 00 00 f3 16 ba e7 98 d7 21 cd 74 09 58 a3 20 f9 58 def6d6df391524ed23...
  0030 58 de f6 d6 df 39 15 24 ed 23 77 fd 33 74 9e fa 58 def6d6df391524ed23...
  0040 3e 3a da b2 4b 9d f9 71 d0 32 2d f9 ee ca 74 eb 58 def6d6df391524ed23...
  0050 45 b9 2b 37 f9 77 2d 7b ab b4 44 ae 9c 30 30 0c 58 def6d6df391524ed23...
  0060 c9 18 7c 01 a4 58 37 13 16 9f f0 e5 4c a2 65 b5 58 def6d6df391524ed23...
  0070 cb b5 5b c9 e2 4f 55 ff 98 2f c3 79 7f 6f 83 1d 58 def6d6df391524ed23...
  0080 30 63 e8 48 b1 d0 25 11 2c 8d 37 9c e7 93 44 ce 58 def6d6df391524ed23...
  0090 44 c5 7a a2 d5 5b 4a 3f f7 0f 74 65 81 8f 2c 5d 58 def6d6df391524ed23...
  00a0 5a ad 57 8c 74 8e a2 4d 3d ad 47 d4 1a ba d8 2b 58 def6d6df391524ed23...
  00b0 a8 c1 4f 23 cb a5 82 39 8b 5c 5d 42 1e f7 e7 fa 58 def6d6df391524ed23...
  00c0 50 ff 3a 27 5d ed c2 c3 a4 7e f0 95 e1 a0 a8 fd 58 def6d6df391524ed23...
  00d0 d1 76 d9 d5 23 e7 f8 2d 33 97 4f 18 60 32 4c 4c 58 def6d6df391524ed23...
  00e0 28 50 31 c3 90 ab 4c 4a d4 47 58 20 ba 7e 28 df 58 def6d6df391524ed23...
  00f0 54 a8 6d 39 d2 87 2f 80 80 14 04 23 72 35 77 47 58 def6d6df391524ed23...
  0100 d2 90 d2 20 f2 84 86 f7 6d 91 8c d4 b1 b9 7c 53 58 def6d6df391524ed23...
  0110 3d 95 82 89 58 de c2 65 40 a5 45 db 69 bd f3 ef 58 def6d6df391524ed23...
  
```

Datos cifrados

Envío de datos

Casos prácticos

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



Topología WPA3-Enterprise

Nombre (SSID):	TFG_UOC	Ocultar
Nivel de seguridad:	WPA3-Enterprise	
Introduzca la información del servidor de autenticación		
Dirección IP:	192.168.1.125	
Número de puerto:	1812	
Secreto compartido:	Seguridad*2019*	
Compatibilidad con PMF:	Activado - Obligatorio	

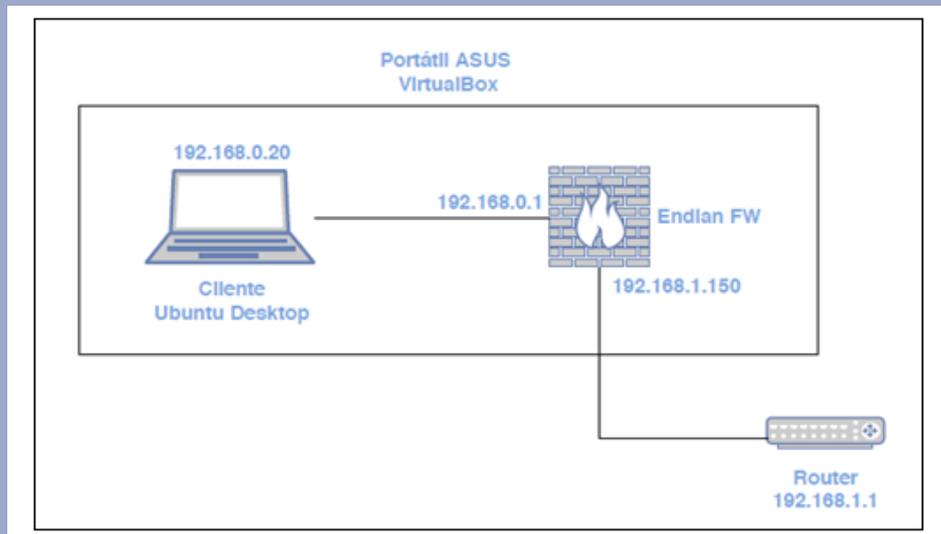
Configuración Router

```
update_config=1
ctrl_interface=/run/wpa_supplicant
ctrl_interface_group=adm
network={
    ssid="TFG_UOC"
    key_mgmt=WPA-EAP-SUITE-B 128 bits
    eap=TTLS
    scan_ssid=1
    ieee80211w=2 PMF
    group_mgmt=BIP-GMAC-256
    ca_cert="/home/cesar/ca.pem"
    identity="usuario"
    password="Seguridad*2019*"
    phase2="auth=MSCHAPV2"
}
```

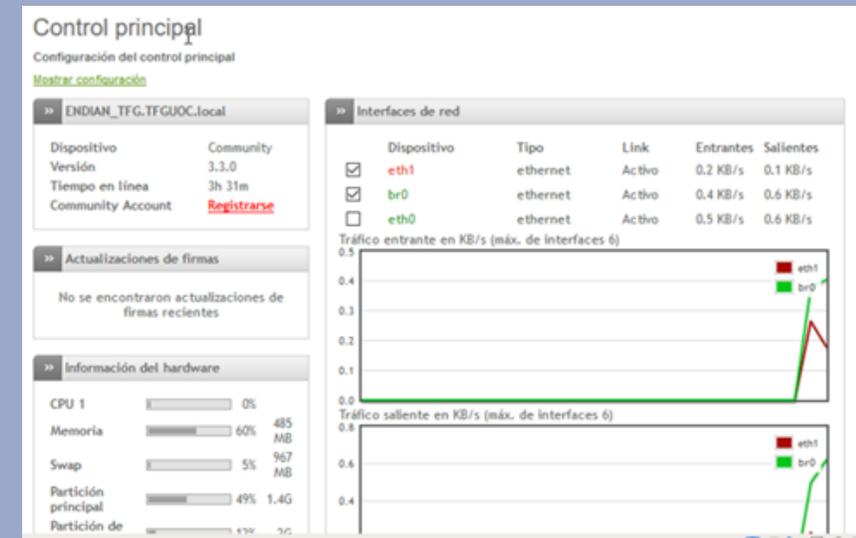
Configuración Cliente

Casos prácticos

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



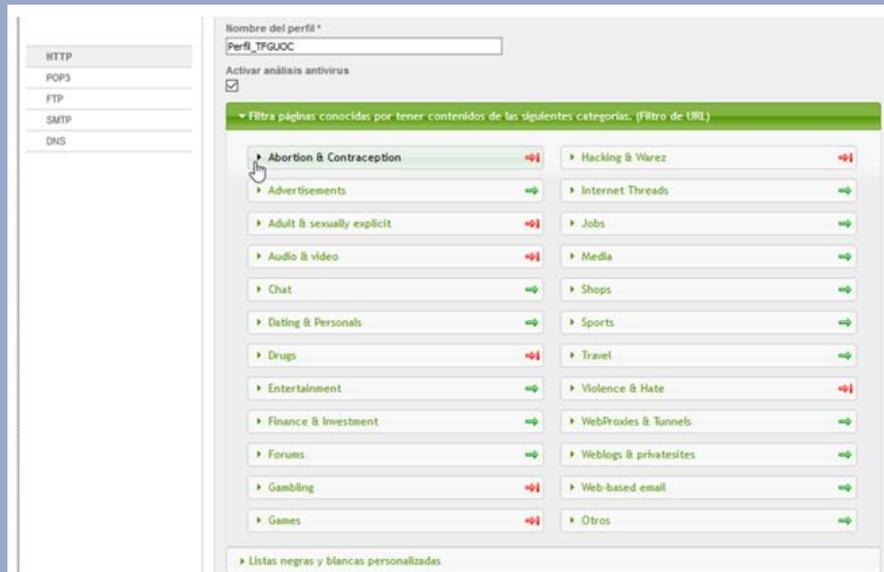
Topología FW UTM



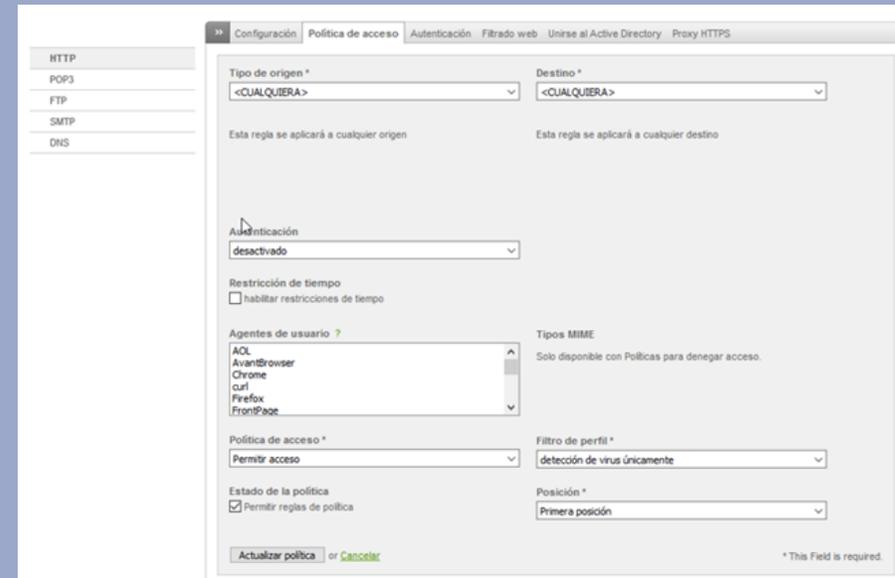
Página Principal

○ 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)

Muchas gracias