CWA para WLAN de invitados integrada con ISE

Comunidad de Cisco

Estefania Pacheco – Wireless Technical Leader TAC
Luis Alberto González – Wireless Technical leader TAC

Martes 5 de Octubre de 2023

Conecte, Interactúe, ¡Colabore!

Soluciones

¡Acepte las soluciones correctas y felicite a quienes le ayudaron! Los foros de discusión tienen muchas entradas, de las cuales no todas cuentan con una respuesta correcta o válida.

Ayude a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución”.

Aceptar como solución

Agradecimientos

¡Resalte el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndoles la oportunidad de ganar premios además de ser una muestra valiosa de ¡nuestro reconocimiento!

0 Útil

Spotlight Awards

¡Nuevos ganadores cada periodo!

Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros. Los Premios Spotlight se otorgan mensualmente cada trimestre para destacar a los miembros más sobresalientes.

¡Ahora también puedes nominar a un candidato! Haga clic aquí

Community Spotlight awards

Estefania Pacheco

Technical Leader Wireless TAC

Con más de cinco años de experiencia en Cisco, Estefania comenzó su carrera en el sector inalámbrico como ingeniera consultora técnica, donde se convirtió en ingeniera de escalamiento y finalmente hizo la transición a su puesto actual. Tiene una licenciatura en ingeniería en telecomunicaciones de la Universidad Nacional Autónoma de México (UNAM) y ha obtenido las certificaciones CCNP R&S y CCNP Wireless.

Luis Alberto González

Technical Leader Wireless TAC

Con más de 13 años de experiencia, Luis tiene un sólido conocimiento en redes inalámbricas, proveedores de servicios de Internet (ISP), gestión de operaciones de grandes redes y manejo de incidentes y escaladas. Le apasiona el tema de la virtualización y su evolución hacia la nube. Se graduó de la Universidad Jesuita de Guadalajara (ITESO) como Ingeniero en Redes y Telecomunicaciones. Actualmente posee las certificaciones CCNP R&S, diseño BELDEN e instalación LEONI.

Descargue la presentación

https://bit.ly/CLdoc-oct23

slido

Join at

slido.com

#7068 161

Passcode: **djdbjs**

Active poll

0

Join at

slido.com

#7068 161

Passcode:

djdbjs

¿Cuál es la mayor preocupación de seguridad que usted cree que podria resolver con CWA?

a) Control en la autenticación de usuarios invitados

0%

b) Fuertes medidas de cifrado y privacidad para usuarios

0%

c) Integración sin problemas con todos los sistemas existentes

0%

d) Rendimiento de la red mejorado

0%

Agenda

1. Introducción
2. Proceso de autenticación web
3. CWA en controladores Catalyst 9800
4. Túnel de movilidad: Foreign-Anchor
5. Diagnóstico y resolución de problemas
6. Demostración

1. Introducción

Introducción
Proceso de autenticación web
CWA en controladores Catalyst serie 9800
Túnel de movilidad: Foreign-Anchor
Diagnóstico y resolución de problemas
Demo

¿Qué es CWA?

CWA: Central Web Authentication / Autenticacion Web Central

Solución de autenticación y control de acceso basada en web

Funciones:

- Control de acceso avanzadas
- Políticas de acceso basadas en roles
- Autenticación multifactor
- Auditoría de actividades de usuario

2. Proceso de autenticación web

Introducción

Proceso de autenticación web

CWA en controladores Catalyst serie 9800

Túnel de movilidad: Foreign-Anchor

Diagnóstico y resolución de problemas

Demo

Tipos de autenticación web

- Local Web Auth (LWA)
  - Utiliza la página web interna del controlador
  - La página web puede ser personalizada utilizando el Webauth Bundle de cisco.com

- Central Web Auth (CWA)
  - ISE hospeda la página web y autentica a los clientes
  - Solución Cisco

- External Web Auth (EWA)
  - Un servidor externo hospeda la página web
  - Solución de terceros
  - Solución Cisco Spaces
    Mas información: DNA Spaces Captive Portal with Catalyst 9800 WLC

¿Cómo funciona CWA?

Es un proceso de Autenticación de Capa 3 que integra uso de un portal web con la técnica de control de acceso MAB

El cliente se asocia a un Access Point → El cliente obtiene una Dirección IP e información del servidor DNS → El cliente inicia una conexión hacia una dirección URL → El cliente envía una consulta de DNS (DNS Query) → DNS Server resuelve el URL en una dirección IP y responde al cliente. → Para abrir la página, el cliente envía un HTTP GET a la IP resuelta → El WLC intercepta el HTTP GET y responde con un REDIRECT con el URL del portal web de ISE → El cliente verá el portal de autenticación de ISE donde podrá presentar sus credenciales o registro.

¿Cómo funciona CWA?

Una vez autenticado el cliente, opcionalmente se podría redireccionar nuevamente a alguna otra página especificada.

No es necesario instalar certificado en el controlador

La máquina de estados en un RA trace de cliente se puede ver:

IOS-XE

S_CO_INIT → S_CO_ASSOCIATING → S_CO_MACAUTH_IN_PROGRESS → S_CO_L2_AUTH_IN_PROGRESS → S_CO_IP_LEARN_IN_PROGRESS → S_CO_L3_AUTH_IN_PROGRESS → **S_AUTHIF_WEBAUTH_PENDING** → **S_AUTHIF_WEBAUTH_DONE** → S_CO_RUN

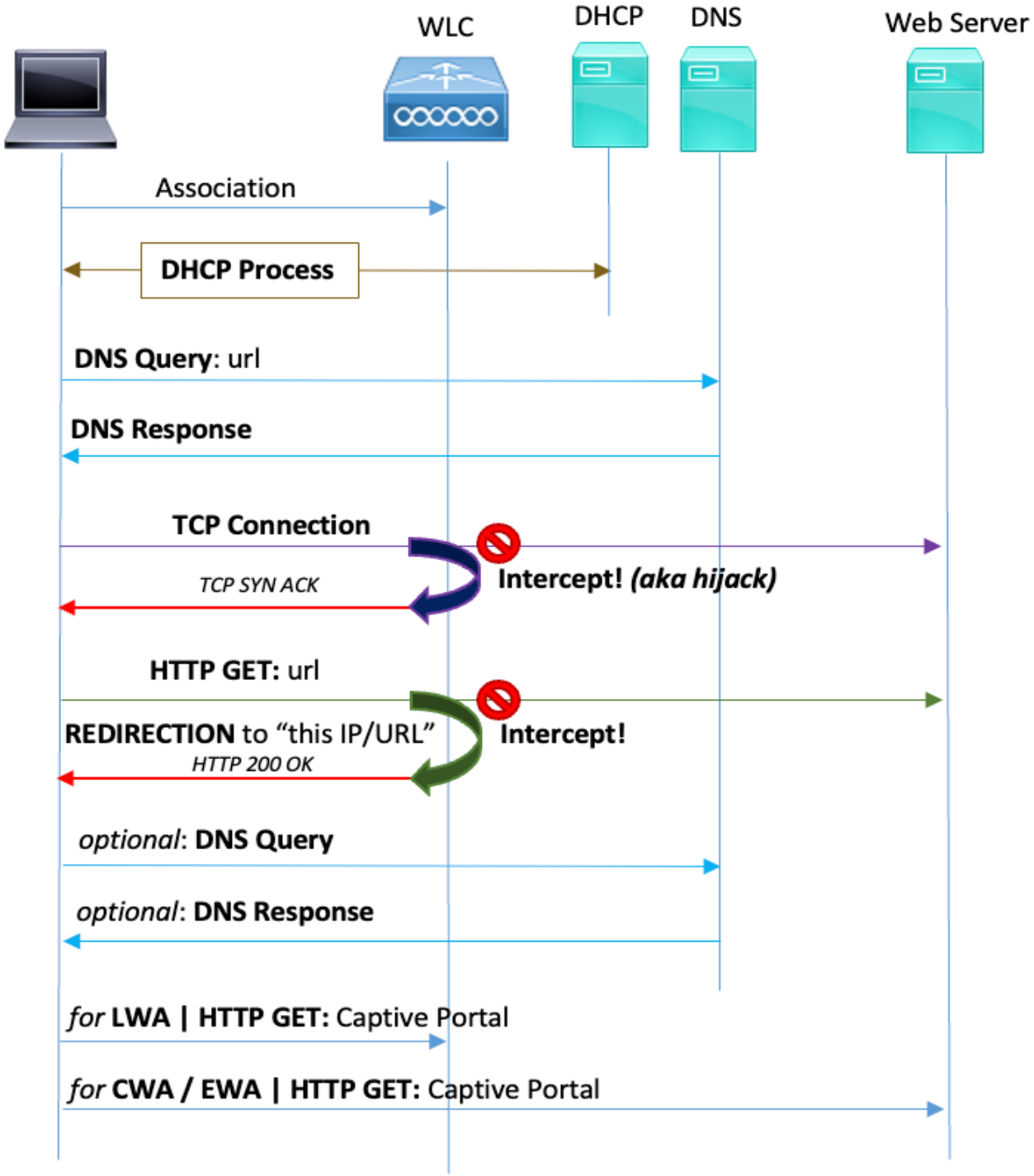


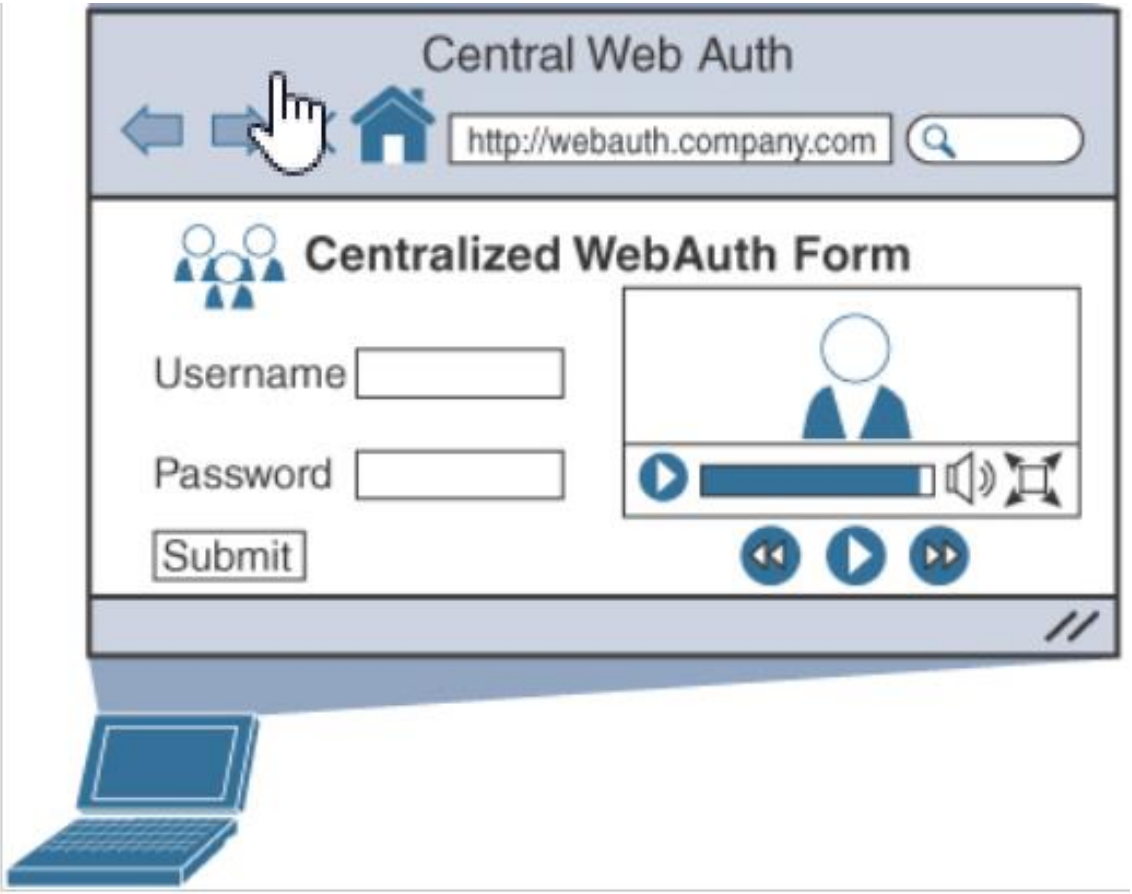
Diagrama funcional de alto nivel

Importante

- ✓ El servidor DNS debe poder resolver URLs de Internet
- ✓ Sin DNS Query Response, no habrá conexiones TCP
- ✓ Sin conexiones TCP no habrá HTTP-GET
- ✓ Sin HTTP-GET no hay Redireccion
- ✓ Sin Redireccion no hay Portal

WEBAUTH_PENDING

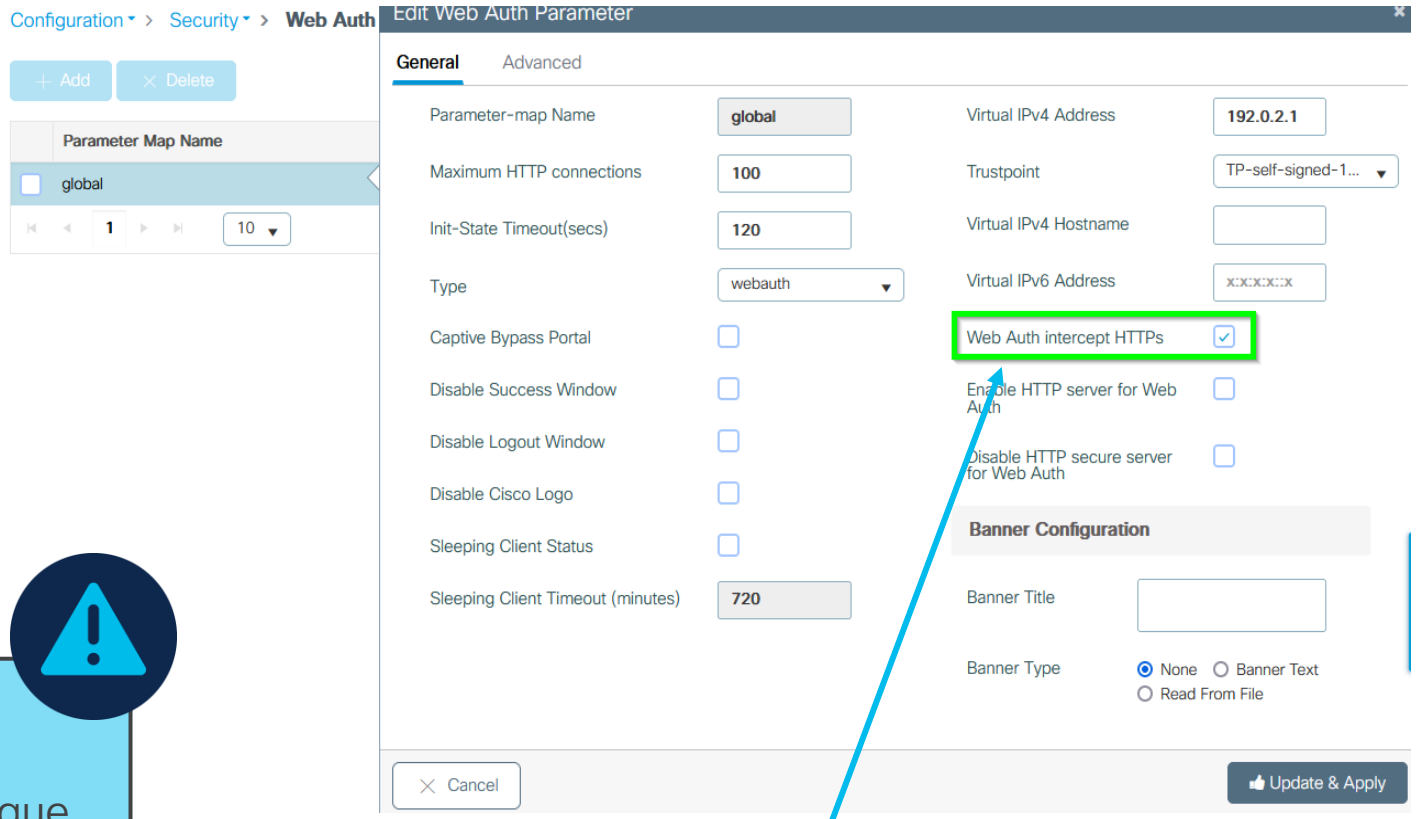
- Normalmente, cuando hay un problema de webauth, los clientes quedan atrapados en este estado.
- Desde la perspectiva del controlador, está esperando que el cliente sea autenticado en la página web.
- Sin embargo, es posible que el cliente no vea el portal web...



Redirección HTTPS

Si el cliente consulta una dirección de tipo HTTPS entonces enviara un **HTTPS-GET.**

Por defecto controlador no está configurado para interceptar tráfico HTTPS por lo que la redirección HTTPS no ocurrirá.



Importante

- La redirección HTTPS **NO se recomienda** ya que requiere un uso intensivo de CPU y genera error de certificado.
- Se recomienda usar solo Redirección HTTP.

Si lo necesita habilite la intercepción de HTTPS para habilitar esta característica.

Redirección: HTTP o HTTPS

Para proceder con la REDIRECCIÓN el controlador necesita **interceptar** ya sea el **HTTP-GET** o **HTTPS-GET** del cliente.

Requisito habilitar:

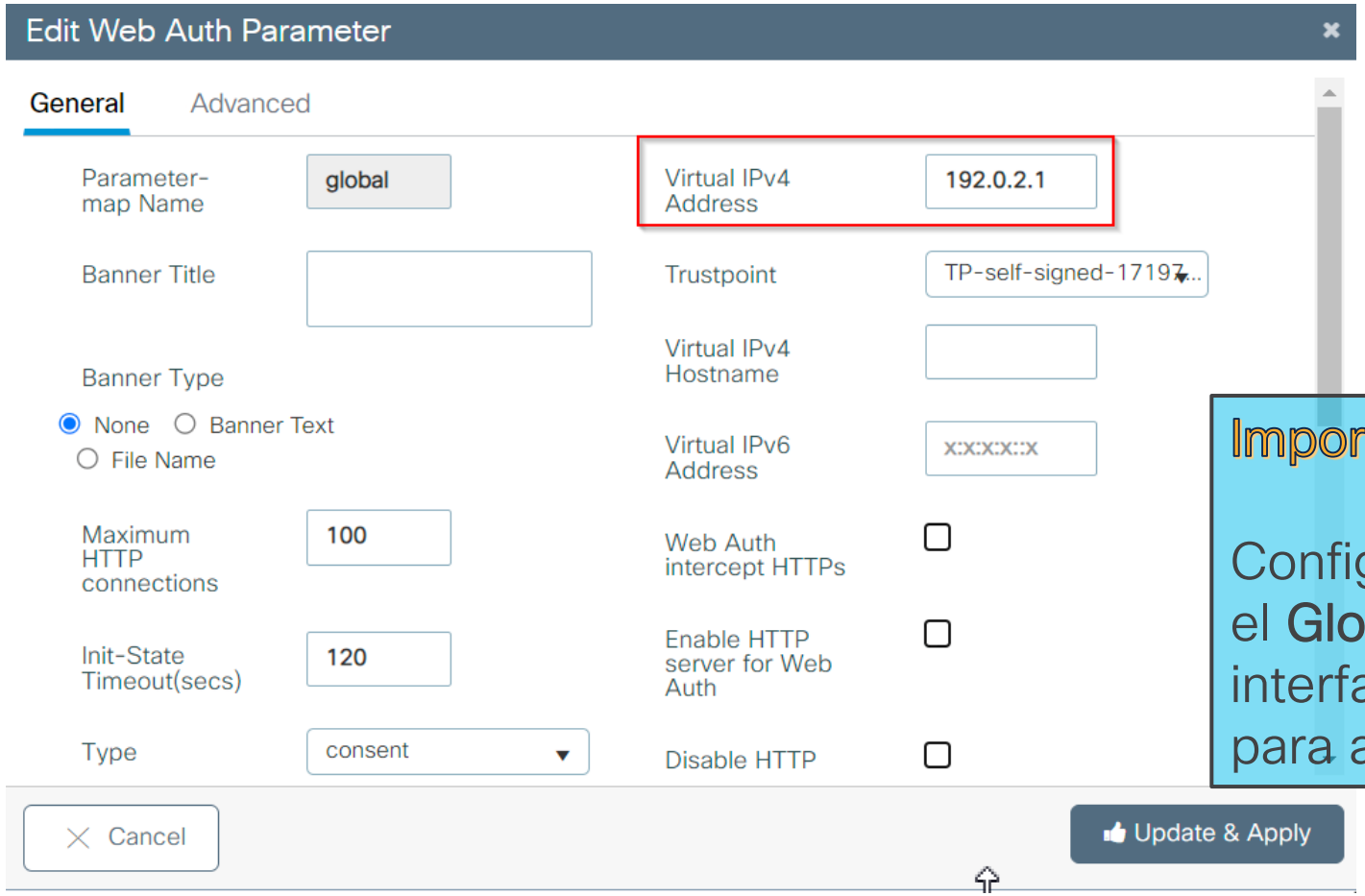
- HTTP → `ip http server`
- HTTPS → `ip http secure-server`

[Configuring HTTP and HTTPS Requests for Web Authentication]

```
http.request.method == "GET"

No.   Time        Stream index  Source        Destination     Info
2214  28.256494   20            192.168.0.22  172.226.111.8   GET / HTTP/1.1

> Frame 2214: 1102 bytes on wire (8816 bits), 1102 bytes captured (8816 bits) on interface 0
> Ethernet II, Src: IntelCor_52:a9:ea (44:85:00:52:a9:ea), Dst: ArrisGro_2b:e7:e9 (f8:2d:c0:2b:e7
> Internet Protocol Version 4, Src: 192.168.0.22, Dst: 172.226.111.8
> Transmission Control Protocol, Src Port: 55603, Dst Port: 80, Seq: 1, Ack: 1, Len: 1048
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: www.nfl.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0\r
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    > [truncated]Cookie: AMCV_F75C3025512D2C1D0A490D44%40AdobeOrg=-1891778711%7CMCIDTS%7C17612%7C
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.nfl.com/]
    [HTTP request 1/1]
    [Response in frame: 2216]
```

Virtual IP

Configuration > Security > **Web Auth > global**



Importante

Configure la **IP virtual** (Virtual IP, VIP) en el **Global Parameter Map** por que esta interfaz es la que el controlador utiliza para activar el redirect.

Virtual IP | Consideraciones

Debe ser una dirección **no enrutable**

NO utilice la IP **1.1.1.1** ni alguna de las direcciones 1.0.0.0/8 en la **interfaz virtual**

La IP debe seguir el RFC 5737

- 192.0.2.0/24
- 198.51.100.0/24
- 203.0.113.0/24

Active poll

0

Join at

slido.com

#7068 161

Passcode:

djdbjs

¿Cuál es el propósito principal que usted le daria a CWA en su organizacion?

a) Mejorar el rendimiento de la red

0%

b) Proporcionar acceso gratuito a Internet para todos los usuarios

0%

c) Centralizar la autenticación de usuarios y el control de acceso a la red

0%

d) Aumentar la complejidad de la red

0%

3. CWA en controladores Catalyst 9800

Introducción

Proceso de autenticación web

CWA en controladores Catalyst serie 9800

Túnel de movilidad: Foreign-Anchor

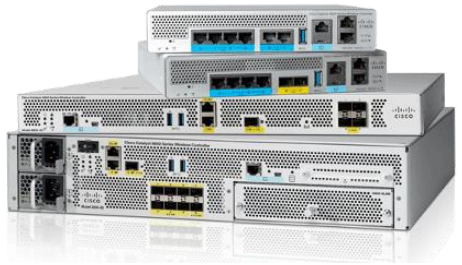
Diagnóstico y resolución de problemas

Demo

Configuraciones para CWA

Configuración en C9800

- Configuración AAA
- CWA en Central Switching
  - Configuración WLAN
  - Configuración Policy profile
  - ACL de redirección
- CWA en Flexconnet Local Switching
  - Policy Profile
  - ACL redirección



Configuración en ISE

- Agregar WLC a Network Devices
- Crear credenciales de usuario
- Crear Autorization Profile para Redirección
- Configurar política de Autenticación (MAB)
- Crear Reglas de Autorización : Permit y Redirect

C9800 | Configuración AAA

- Agregar el servidor ISE a la configuración de 9800

```
aaa new-model
radius server ISE_luis
address ipv4 172.16.48.196 auth-port 1812 acct-port 1813
key Cisco123
aaa group server radius GROUP_RADIUS
server name ISE_luis
```

ISE
172.16.48.196

- Asegurar que el soporte de CoA este habilitado

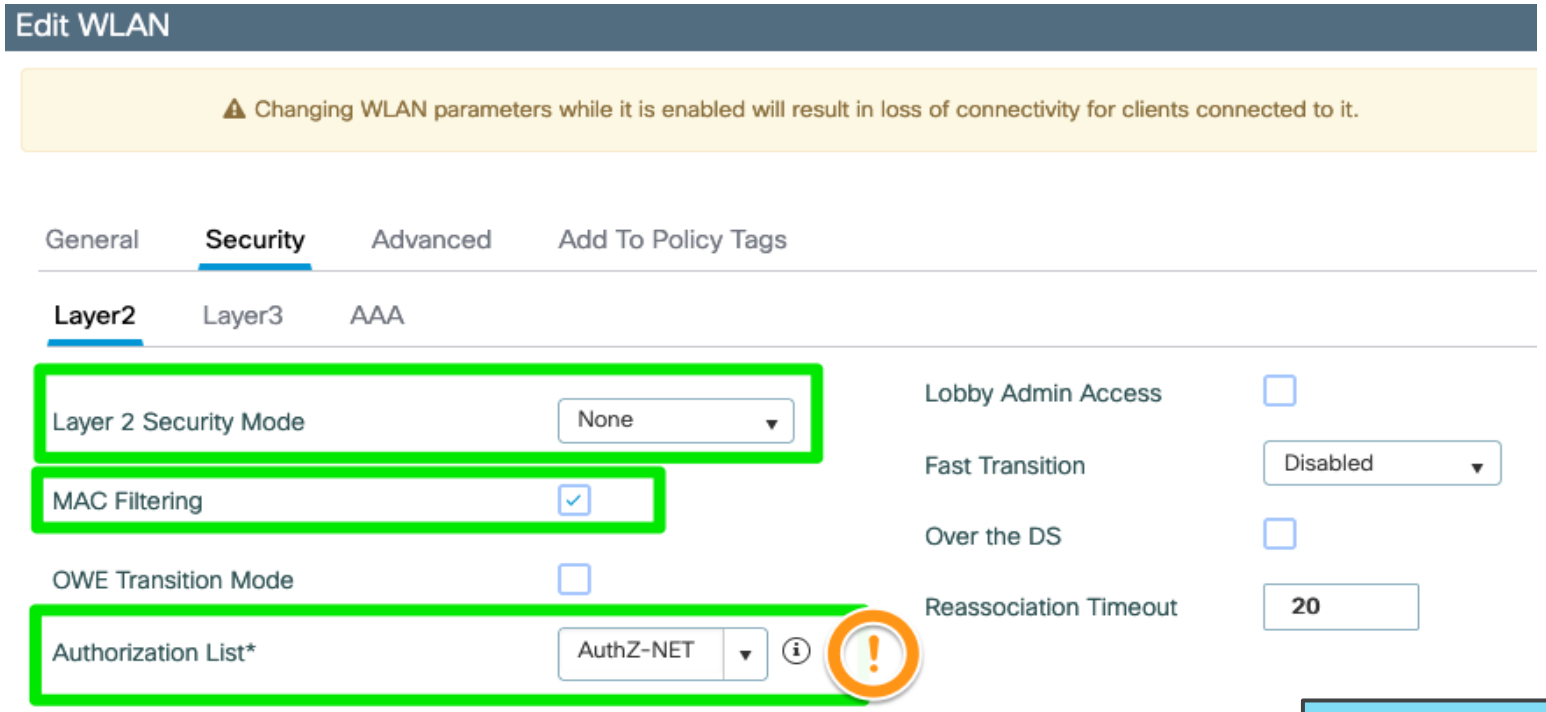
```
aaa server radius dynamic-author
client <ISE-IP> server-key Cisco123
```

- Cree una lista de métodos de Autorización
  y una lista de Accounting (opcional)

```
aaa authorization network AuthZ-NET group GROUP_RADIUS
aaa accounting identity ACC-NET start-stop group GROUP_RADIUS
```

C9800 | Configuración de WLAN

Configuration > Tags & Profiles > WLANS > **+Add**

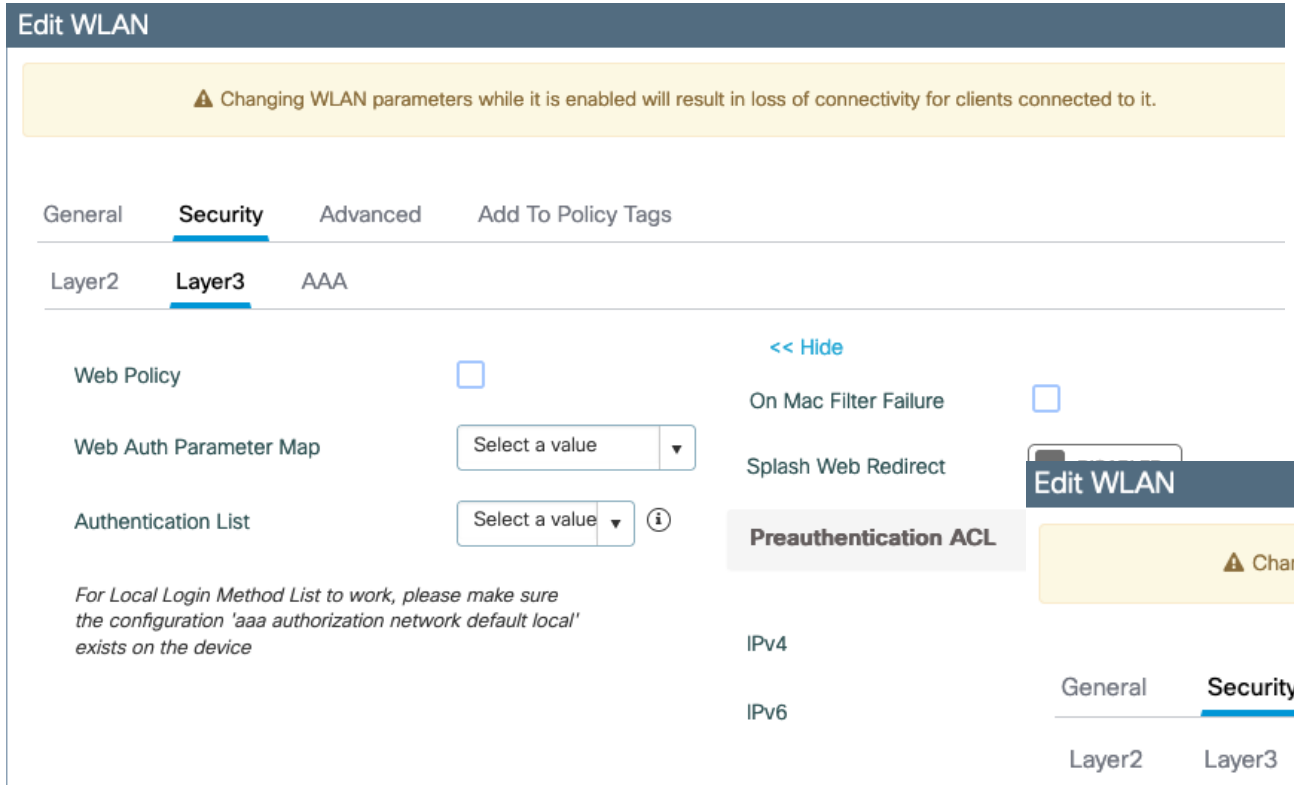


Importante

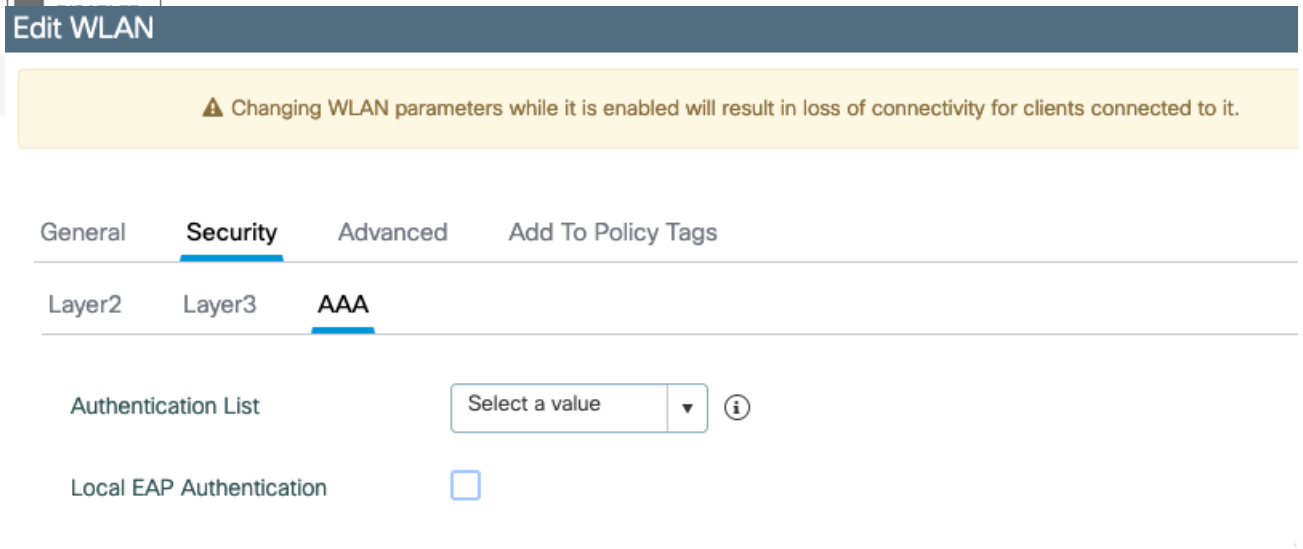
- Con CWA ¡No se necesita una lista de autenticación!
- Sólo **lista de autorización**

C9800 | Configuración de WLAN

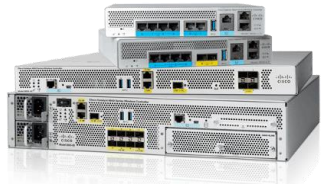
Configuration > Tags & Profiles > WLANS > **+Add**



Nota: No es necesario configurar las pestañas de **Layer 3** y **AAA**



C9800 | Configuración del Policy Profile



Central Switching

Configuration > Tags & Profiles > Policy > **+Add**

Edit Policy Profile

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General | Access Policies | QOS and AVC | Mobility | Advanced

Name*	Normal-Policy-Profile
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
Encrypted Traffic Analytics	DISABLED
CTS Policy	
Inline Tagging	☐
SGACL Enforcement	☐
Default SGT	2-65519

WLAN Switching Policy	
Central Switching	ENABLED
Central Authentication	ENABLED
Central DHCP	ENABLED
Central Association	ENABLED
Flex NAT/PAT	DISABLED

Edit Policy Profile

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General | Access Policies | QOS and AVC | Mobility | Advanced

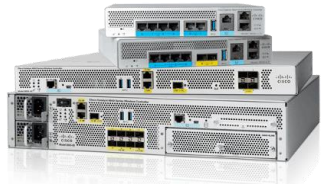
RADIUS Profiling	☐
HTTP TLV Caching	☐
DHCP TLV Caching	☐
WLAN Local Profiling	
Global State of Device Classification	Disabled ⓘ
Local Subscriber Policy Name	Search or Select
VLAN	
VLAN/VLAN Group	2650
Multicast VLAN	Enter Multicast VLAN

WLAN ACL	
IPv4 ACL	Search or Select
IPv6 ACL	Search or Select
URL Filters	
Pre Auth	Search or Select
Post Auth	Search or Select

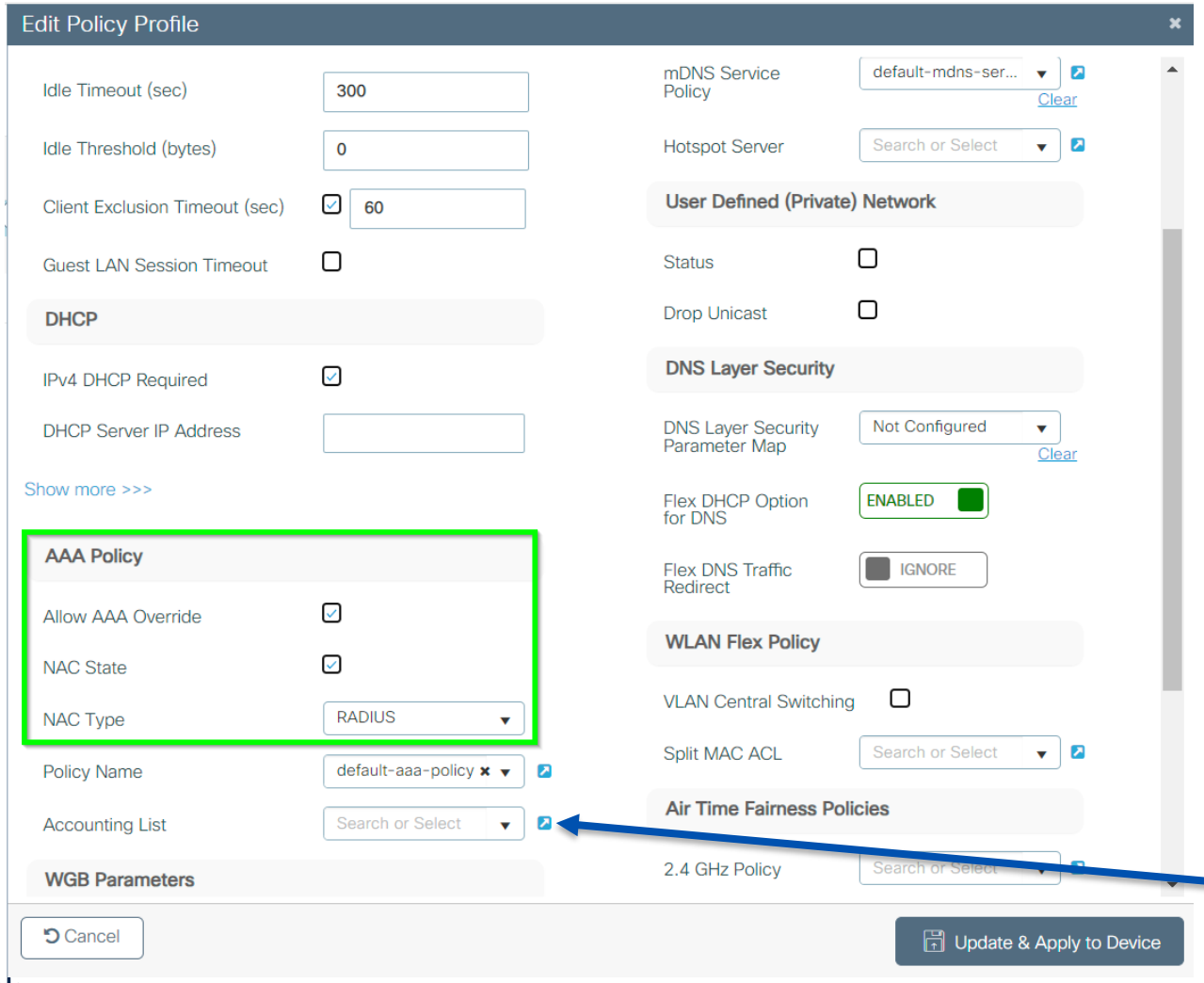
Importante

- CWA en *Flexconnect local switching* es possible

C9800 | Configuración del Policy Profile



Configuration > Tags & Profiles > Policy > **Advanced**



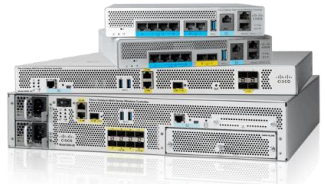
Después de configurar el WLAN profile y Policy Profile agregue este mapeo a su Policy Tag

Configuration > Tags & Profiles > Tags > **Policy**

Importante

- **Accounting List** es Opcional
  Mas informacion: Radius Accounting

C9800 | ACL de Redirección



Configuration > Security > **ACL**

Edit ACL

ACL Name*	CWA-ACL	ACL Type	IPv4 Extended

Rules

Sequence*		Action	permit
Source Type	any		
Destination Type	any		
Protocol	ahp		
Log	☐	DSCP	None

+ Add × Delete

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP
☐	10	deny	any		any		udp		eq bootps	None
☐	20	deny	any		any		udp	eq bootpc		None
☐	30	deny	any		any		udp		eq domain	None
☐	40	deny	any		any		udp	eq domain		None
☐	50	deny	any		172.16.48.196		ip			None
☐	60	deny	172.16.48.196		any		ip			None
☐	70	permit	any		any		ip			None

1 | 10 items per page 1 - 7 of 7 ite

ISE
172.16.48.196

- En 9800 se redirecciona con **permit**
- El nombre de la ACL debe ser exactamente igual en ISE
- La configuración de ISE se mantiene

```
ewlc#show ip access-lists CWA-ACL
Extended IP access list CWA-ACL
10 deny udp any any eq bootps
20 deny udp any eq bootpc any
30 deny udp any any eq domain
40 deny udp any eq domain any
50 deny ip any host 172.16.48.196
60 deny ip host 172.16.48.196 any
70 permit ip any any
```

C9800 | ACL de Redirección… ¿HTTPS?

```
ewlc#show ip access-lists CWA-ACL
Extended IP access list CWA-ACL
10 deny udp any any eq bootps
20 deny udp any eq bootpc any
30 deny udp any any eq domain
40 deny udp any eq domain any
50 deny ip any host 172.16.48.196
60 deny ip host 172.16.48.196 any
70 permit ip any any
```

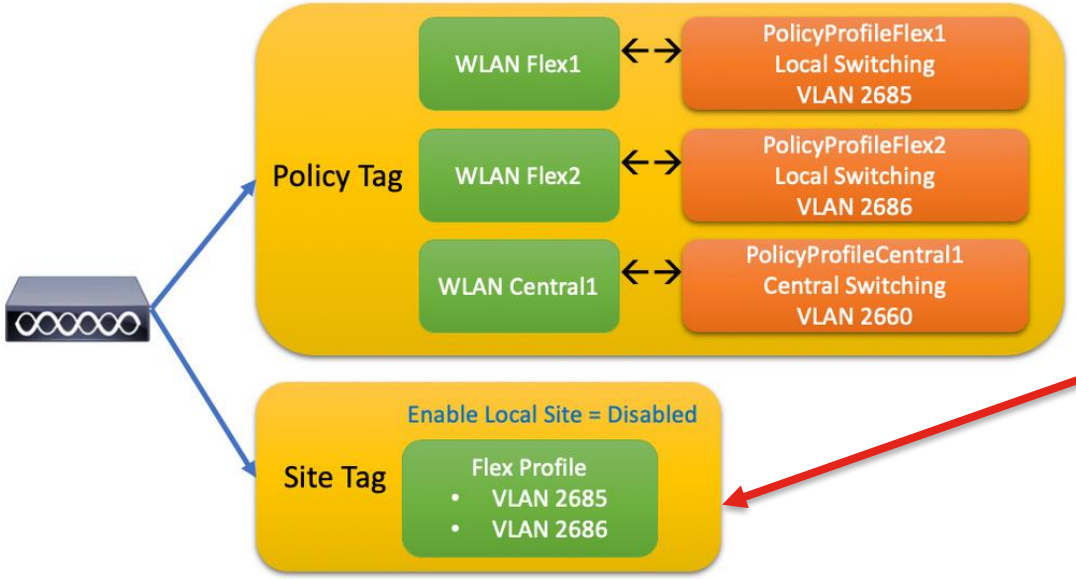
Esta entrada de la lista de acceso redirigirá TODO el tráfico, incluido HT TPS

Sin embargo, sabemos que redirigir HTTPS no es deseable (la mayoría de las veces), por lo que es posible que debamos modificar esa entrada para redirigir solo HTTP con:

```
70 permit tcp any any eq 80
```

C9800 | CWA en **Flexconnect**

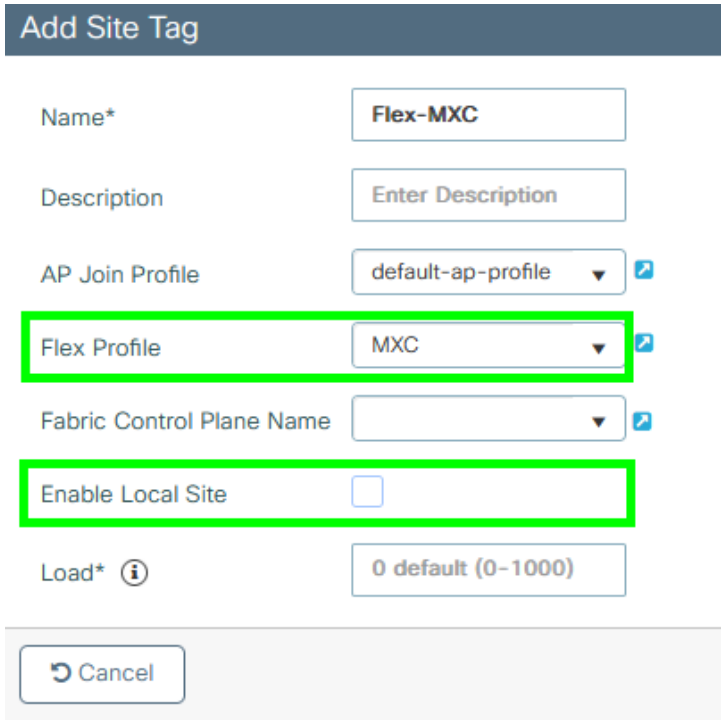
Local Switching



Configuraciones Flexconnect:

En el **Site Tag** tendrá que desmarcar "Enable local site“ y asignar un Flex Profile

Configuration > Tags & Profiles > Tag > **Site**

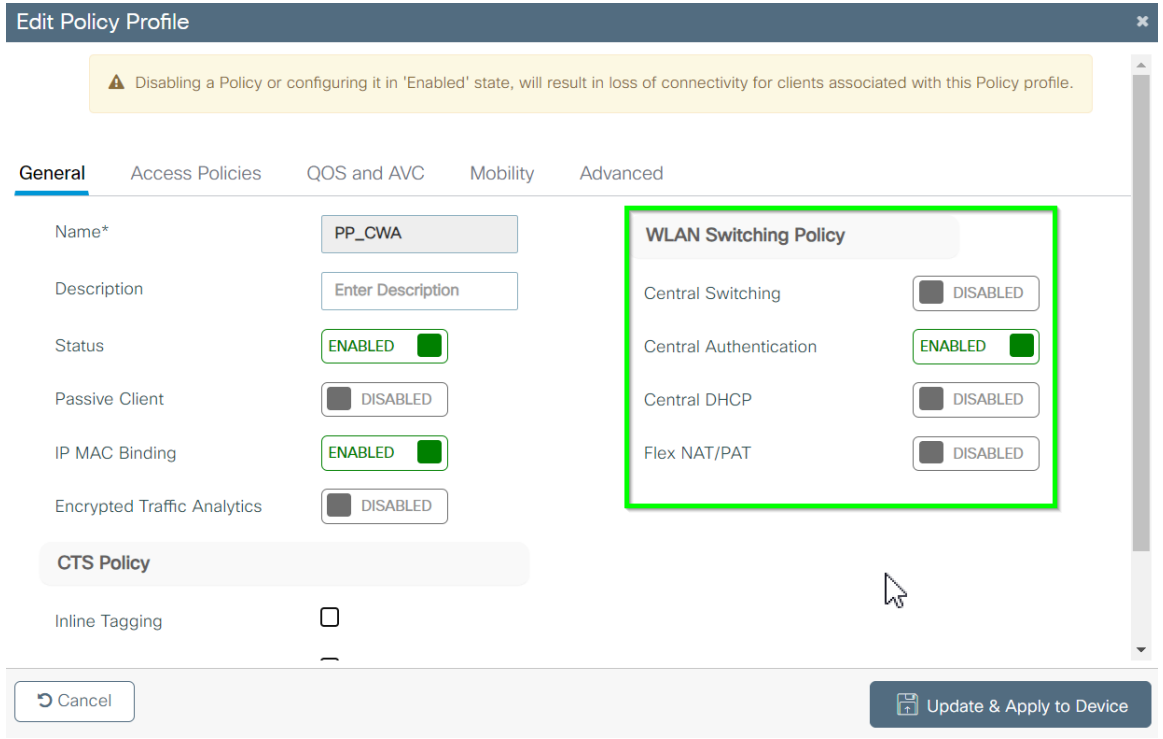


El **WLAN profile y** el mapeo de **Policy Tag** mantienen la misma configuración que en la implementación centralizada.

C9800 | CWA en **Flexconnect**

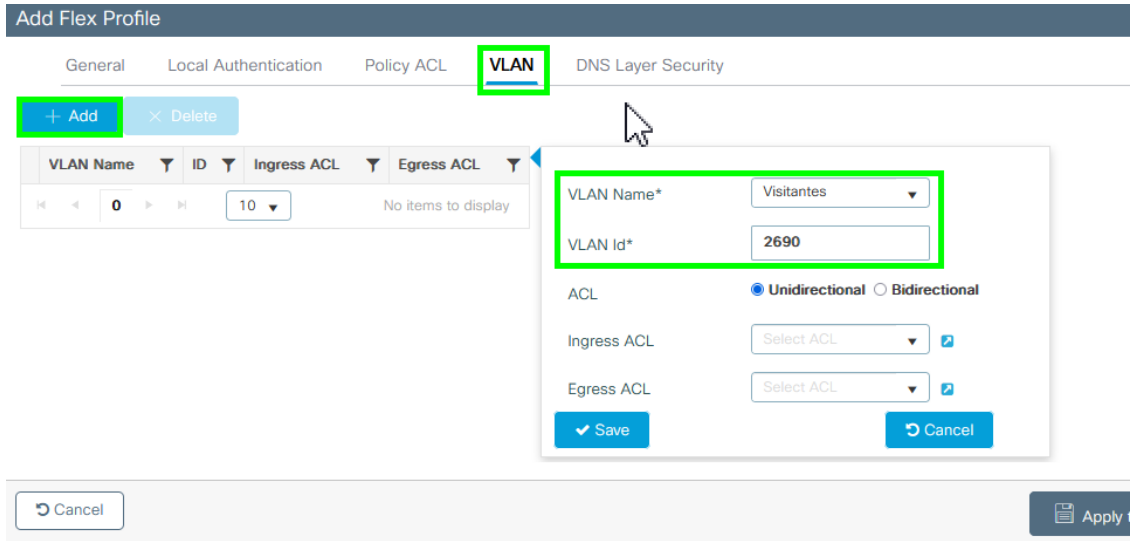
Local Switching

Configuration > Tags & Profiles > Policy > General



- Configure el **Flex profile** con la asignación de VLAN adecuada.

Configuration > Tags & Profiles > **Flex**



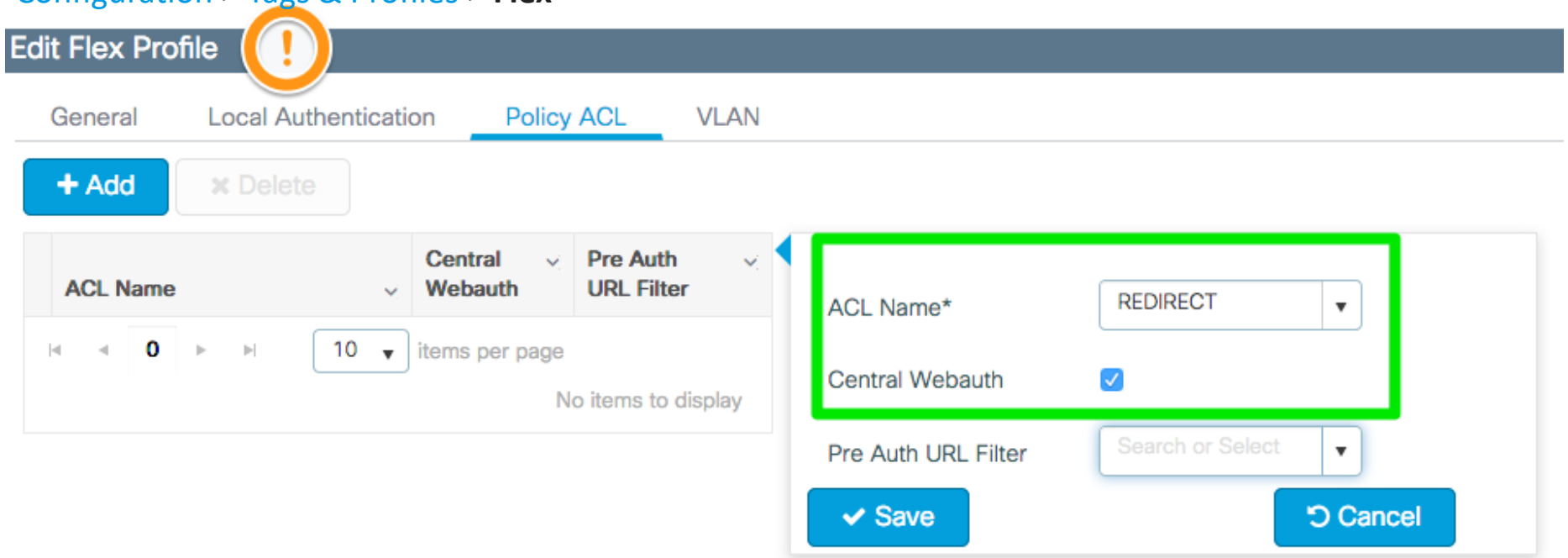
- Configurar **Policy Profile** en **local switching** al deshabilitar “Central Switching”

C9800 | CWA en **Flexconnect**

Local Switching

- Entonces para CWA con Flexconnect aquí está el truco:
- En su **Flex Profile**, debe enviar la ACL de redirección a los AP.
- ¿Cómo? Seleccionando la ACL y habilitando **Central WebAuth**

Configuration > Tags & Profiles > **Flex**



C9800 | Configuración en CLI | Central Switching

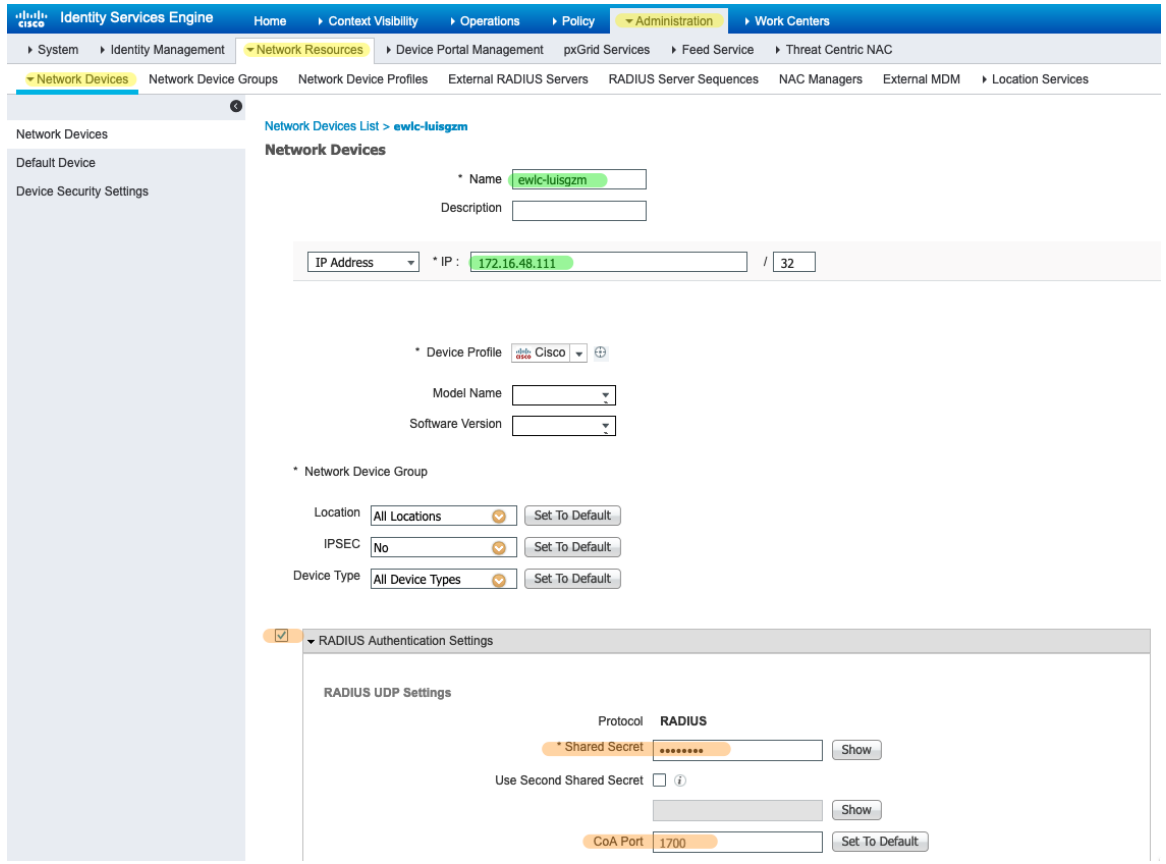
```
aaa new-model

aaa group server radius GROUP_RADIUS
server name ISE3_luis

aaa authorization network AuthZ-NET group GROUP_RADIUS

aaa server radius dynamic-author
client 172.16.48.196 server-key Cisco123

wireless profile policy POLICY_CWA
aaa-override
no exclusionlist
nac
vlan 2649
no shutdown

wlan L-CWA-9800 2 L-CWA-9800
mac-filtering AuthZ-NET
no security ft adaptive
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no shutdown
```

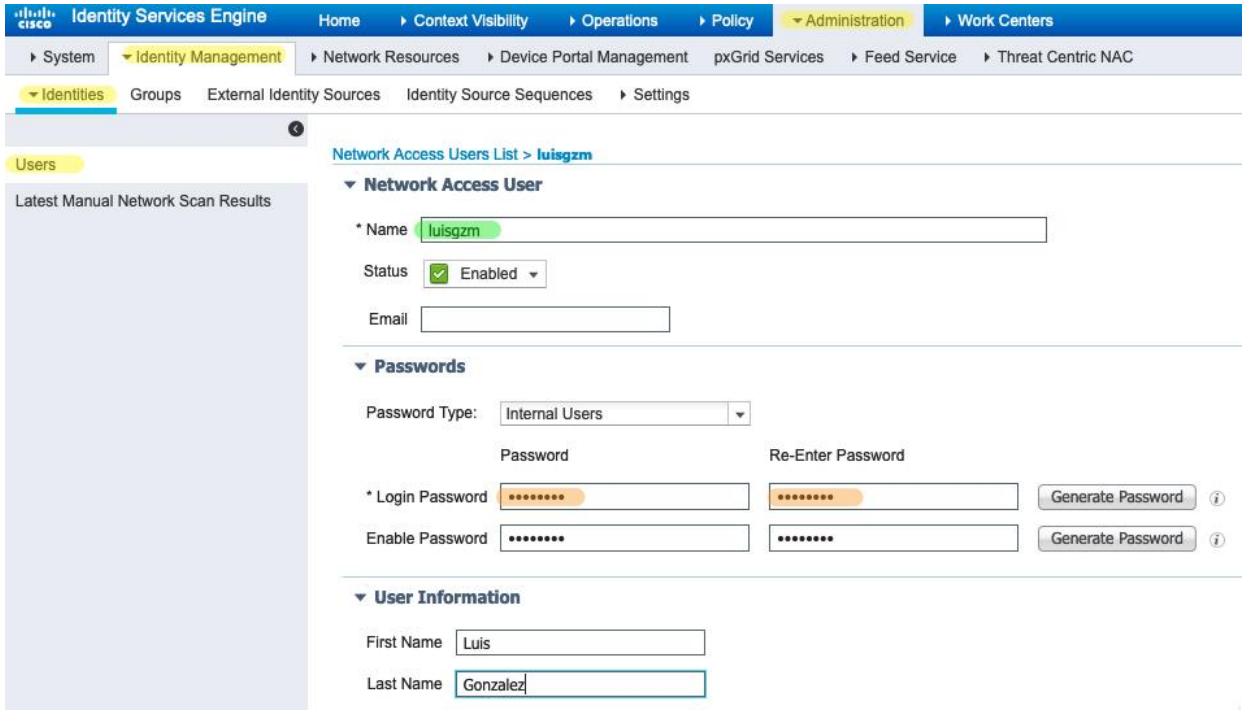
```
ip access-list extended CWA-ACL
10 deny   udp any any eq bootps
20 deny   udp any eq bootpc any
30 deny   udp any any eq domain
40 deny   udp any eq domain any
50 deny   ip any host 172.16.48.196
60 deny   ip host 172.16.48.196 any
70 permit ip any any

radius server ISE3_luis
address ipv4 172.16.48.196 auth-port 1812 acct-port 1813
key Cisco123

parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 intercept-https-enable

ip http server
ip http secure-server
```

Nota: Configuración parcial que solo muestra los fragmentos más relevantes. Corresponde a CWA Central Switching.

ISE | Configuraciones preliminares

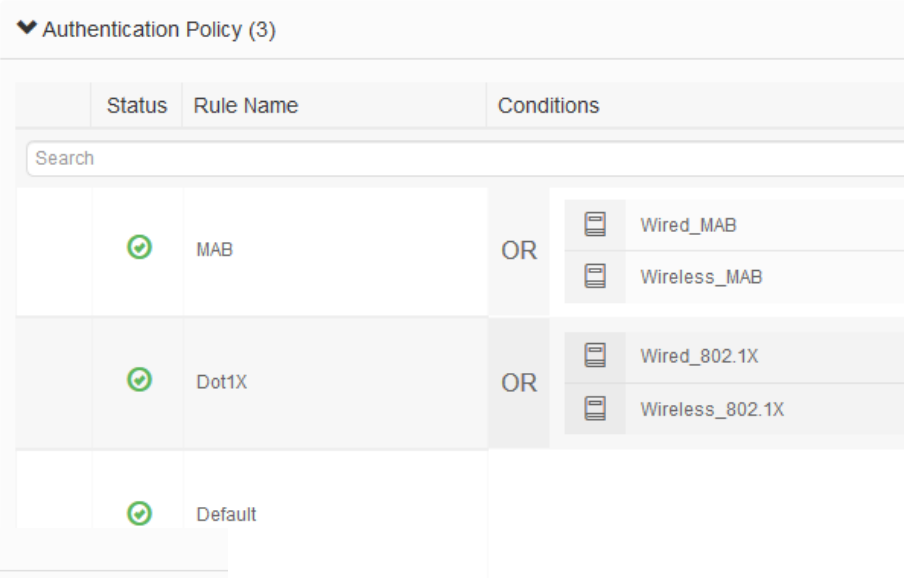
La WLC y los usuarios deben agregarse en ISE (igual que en 802.1x)

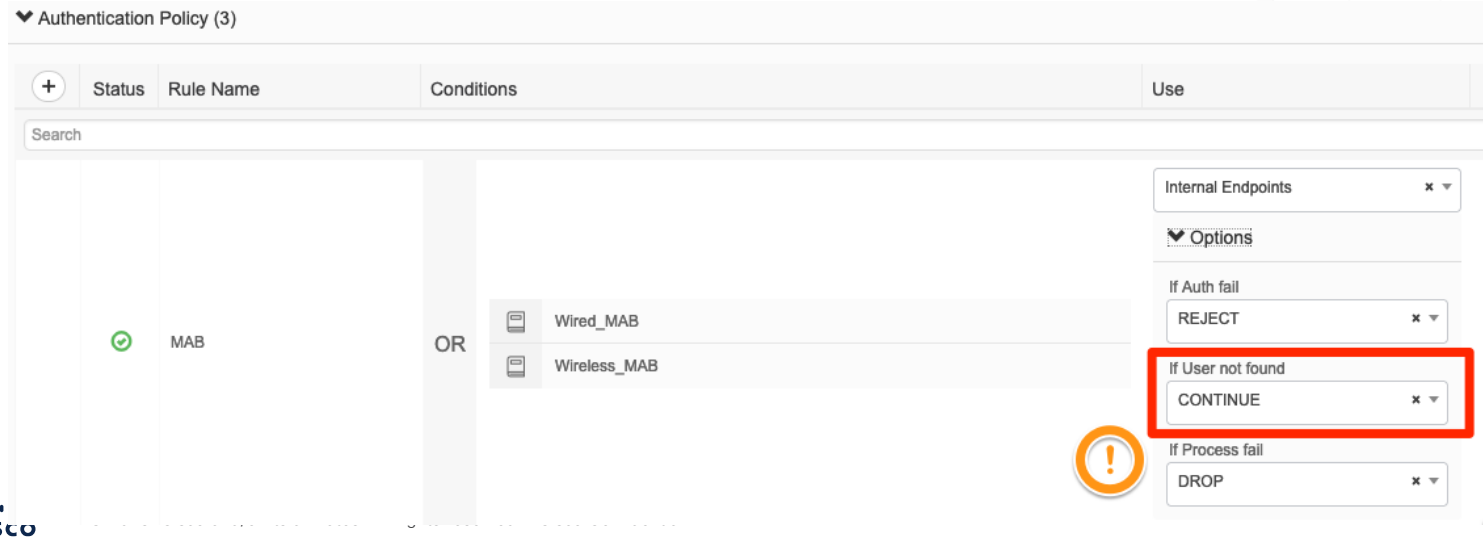




CWA & ISE: Política de Autenticación (MAB)

Dado que la WLAN tiene habilitado el **Filtrado MAC**, enviaremos el **Calling-Station-ID** al servidor AAA, coincidiendo con la regla MAB.





Específicamente para MAB, asegúrese de tener **CONTINUE** en “If user not found”

CWA & ISE: Reglas de Autorización

Necesitamos crear al menos dos reglas en el siguiente orden:

1. **Regla PERMIT**: Enviará un **PermitAccess** una vez que se haya completado todo el proceso.
2. **Regla REDIRECT**: Enviará la **REDIRECCIÓN** (a la página web)

L-CWA-Permit	Guest_Flow	× PermitAccess	+
L-CWA-Redirect	Radius·Called-Station-ID CONTAINS L-CWA	× CWA-Redirect	+

ISE evalúa las reglas de manera secuencial: **de arriba a abajo**

Importante

- Cuando la conexión es nueva primero coincidiremos con la regla **REDIRECT**.
- Después del CoA, coincidiremos con la regla **PERMIT**.

CWA & ISE:

Authorization Profile

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Dictionaries | Conditions | Results

- Authentication
- Authorization
  - Authorization Profiles
  - Downloadable ACLs
- Profiling
- Posture
- Client Provisioning

Authorization Profile

* Name: CWA-Redirect

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: ☐

Track Movement: ☐

Passive Identity Tracking: ☐

Common Tasks

☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth | ACL: CWA-ACL | Value: istered Guest Portal (default)

☑ Display Certificates Renewal Message

☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for endpoints in Logical Profile

Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=CWA-ACL
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=aa0f16f0-4b97-11e7-bfd8-005056aba474&daysToExpiry=value&action=cwa
```

Esto es lo que ISE envía con la regla REDIRECT

Active poll

0

Join at

slido.com

#7068 161

Passcode:

djdbjs

¿Cuál es una preocupación de seguridad potencial relacionada con la Autenticación Web Central?

A) Vulnerabilidades en la autenticación de usuarios invitados

0%

B) Fuertes medidas de cifrado y privacidad para usuarios

0%

C) Integración sin problemas con todos los sistemas existentes

0%

D) Rendimiento de la red mejorado

0%

4. Túnel de movilidad: Foreign-Anchor

Introducción

Proceso de autenticación web

CWA en controladores Catalyst serie 9800

Túnel de movilidad: Foreign-Anchor

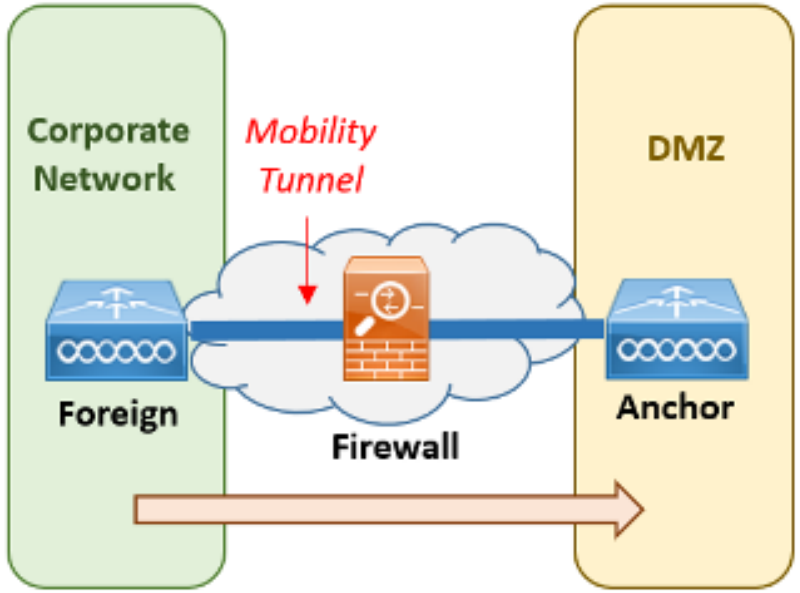
Diagnóstico y resolución de problemas

Demo

CWA… usando Foreign-Anchor

- La idea es mandar todo el tráfico de los Invitado a la **DMZ** a través del tunel de movilidad

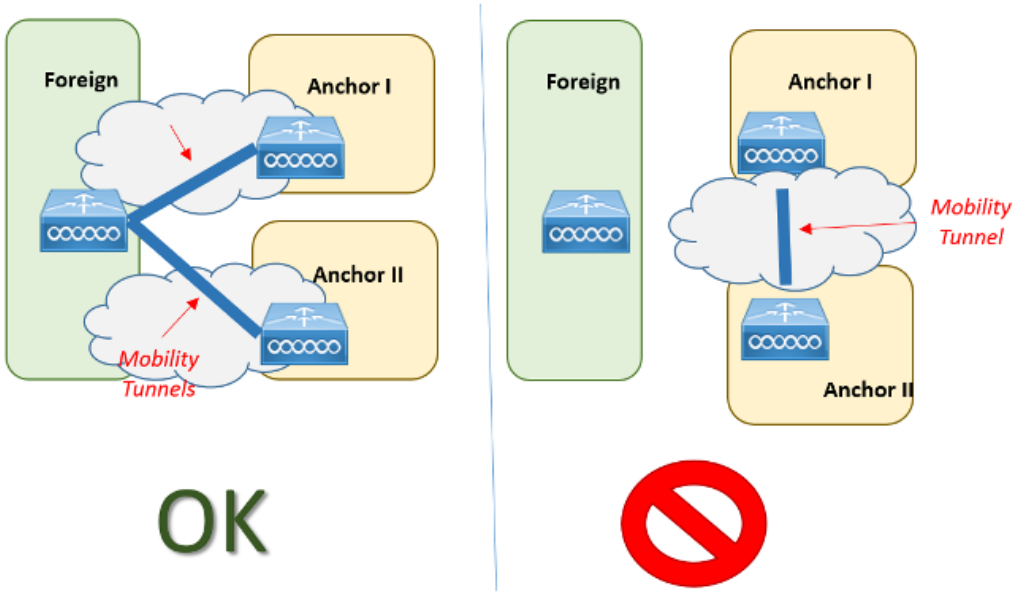
- Recordemos que la DMZ está detrás de un Firewall por lo que no tiene forma de comunicarse con la red Corporativa

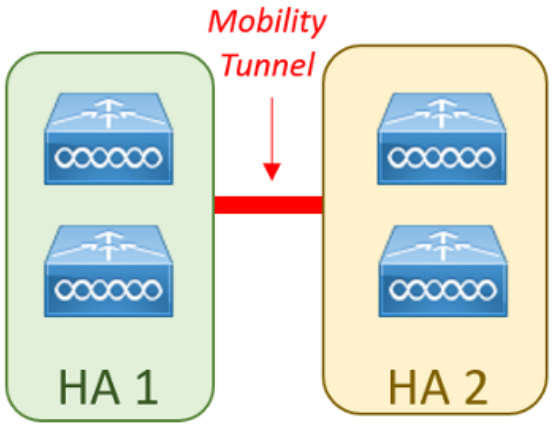


CWA… usando Foreign-Anchor

El túnel de movilidad puede crearse entre controladores **AireOS** y/o **9800**s

Para alta disponibilidad, puede utilizarse una o mas controladores en la DMZ ademas de poder utilizar controladores en HA *(High Availability)*





CWA… usando Foreign-Anchor

Configuration > Wireless > Mobility

Global Configuration | Peer Configuration

Mobility Peer Configuration

+ Add | Delete

MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
001e.e60a.65ff	172.16.48.111	N/A	LUISGZM	224.0.7.111	::	N/A	N/A	539ac63b663baad125e1c7f52d562de6f13df0ff	N/A
001e.e60a.65ff	2001:172:16:48::111	N/A	LUISGZM	224.0.7.111	::	N/A	N/A	539ac63b663baad125e1c7f52d562de6f13df0ff	N/A
001e.e5fb.c7ff	172.16.49.211	172.16.49.211	WEST	0.0.0.0	::	Up	1385	eeab28ae5f531b20b146e852c6c46dbde7d68255	Enabled

1) Creamos nuestros tuneles de movilidad entre controladores

2) En el Policy-Profile asociado a nuestra WLAN, le indicamos que lo Exporte al Anchor con IP 172.16.49.211

Edi Policy Profile

Configuring in enabled state will result in loss of connectivity for clients associated with this profile. There are anchors configured on the policy. Remove anchors before disabling Central Switching.

General | Access Policies | QOS and AVC | Mobility | Advanced

Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)	Selected (1)	
Anchor IP	Anchor IP	Anchor Priority
172.16.48.250	172.16.49.211	Primary (1)

FOREIGN

Ejemplo: Cliente conectado a una WLAN en Foreing-Anchor

Monitoring > Wireless > Clients

Clients | Sleeping Clients | Excluded Clients

Delete

Total Client(s) in the Network: 1

Number of Client(s) selected: 0

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	State	Protocol	User Name	Device Type	Role
e84e.065d.40b4	172.16.49.85	N/A	AP-2802-CALO	eWLC-luisgzm-Anchored	8	Run	11ac		N/A	Export Foreign

1 items per page 10 items per page 1 - 1 of 1 clients

ANCHOR

Monitoring > Wireless > Clients

Clients | Sleeping Clients | Excluded Clients

Delete

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role
e84e.065d.40b4	172.16.49.85	N/A	172.16.48.111	eWLC-luisgzm-Anchored	3	WLAN	Run	N/A		N/A	Export Anchor

1 items per page 10 items per page 1 - 1 of 1 clients

5. Diagnóstico y resolución de problemas

Introducción

Proceso de autenticación web

CWA en controladores Catalyst serie 9800

Túnel de movilidad: Foreign-Anchor

Diagnóstico y resolución de problemas

Demo

ISE | RADIUS Live Logs

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

RADIUS | Threat-Centric NAC Live Logs | TACACS | Troubleshoot | Adaptive Network Control | Reports

Live Logs | Live Sessions

Click here to do visibility setup Do not show this again.

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh Every 10 seconds | Show Latest 100 records | Within Last 24 hours

Refresh | Reset Repeat Counts | Export To | Filter

Time	Status	Details	Repeat Co...	Endpoint P...	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
				Endpoint Profi	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Jul 18, 2023 12:27:04.599 AM			0	Windows10-...	luisgzm	E8:4E:06:5D:40:B4	Default	Default >> CWA_Luis_Accept	PermitAccess	172.16.49.5
Jul 18, 2023 12:27:04.599 AM				Windows10-...	luisgzm	E8:4E:06:5D:40:B4	Default	Default >> CWA_Luis_Accept	PermitAccess	172.16.49.5
Jul 18, 2023 12:27:04.588 AM						E8:4E:06:5D:40:B4				
Jul 18, 2023 12:26:54.128 AM					luisgzm	E8:4E:06:5D:40:B4				172.16.49.5
Jul 18, 2023 12:26:14.009 AM					E8:4E:06:5D:40:B4	E8:4E:06:5D:40:B4	Default >> MAB	Default >> CWA_Luis_Redirect	CWA_Luis	
Jul 18, 2023 12:06:33.065 AM				Microsoft-W...	E8:4E:06:5D:40:B4	E8:4E:06:5D:40:B4	Default >> MAB	Default >> CWA_Luis_Redirect	CWA_Luis	

ISE | Client Report

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	E8:4E:06:5D:40:B4
Endpoint Id	E8:4E:06:5D:40:B4
Endpoint Profile	
Authentication Policy	Default >> MAB
Authorization Policy	Default >> CWA_Luis_Redirect
Authorization Result	CWA_Luis

Authentication Details

Source Timestamp	2023-07-18 00:26:14.009
Received Timestamp	2023-07-18 00:26:14.009
Policy Server	ISE2-luisgzm
Event	5200 Authentication succeeded
Username	E8:4E:06:5D:40:B4
Endpoint Id	E8:4E:06:5D:40:B4
Calling Station Id	e8-4e-06-5d-40-b4
Audit Session Id	CD3110AC000001916663195D
Authentication Method	mab

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15041	Evaluating Identity Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType
15013	Selected Identity Source - Internal Endpoints
24209	Looking up Endpoint in Internal Endpoints IDStore - E8:4E:06:5D:40:B4
24217	The host is not found in the internal endpoints identity store
22056	Subject not found in the applicable identity store(s)
22058	The advanced option that is configured for an unknown user is used
22060	The 'Continue' advanced option is configured in case of a failed authentication request
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
24209	Looking up Endpoint in Internal Endpoints IDStore - E
24217	The host is not found in the internal endpoints identity
15048	Queried PIP - Network Access.UserName
15048	Queried PIP - IdentityGroup.Name
15048	Queried PIP - EndPoints.LogicalProfile
15048	Queried PIP - Network Access.AuthenticationStatus
15048	Queried PIP - Radius.Calling-Station-ID
15048	Queried PIP - Radius.Called-Station-ID
15016	Selected Authorization Profile - CWA_Luis
11002	Returned RADIUS Access-Accept

Result

User-Name	E8-4E-06-5D-40-B4
Class	CACS:CD3110AC000001916663195D:ISE2-luisgzm/472937644/199
cisco-av-pair	url-redirect=https://ISE2-luisgzm.local.com:8443/portal/gateway?sessionId=CD3110AC000001916663195D&portal=f0ae43f0-7159-11e7-a355-005056aba474&action=cwa&token=815991fffcb6ca497be03676e9f9ee4c
cisco-av-pair	url-redirect-acl=CWA_REDIRECT
cisco-av-pair	url-redirect=https://172.16.48.196:8443/portal/gateway?sessionId=CD3110AC000001916663195D&portal=f0ae43f0-7159-11e7-a355-005056aba474&action=cwa&token=6b4912659f97b81b1823e70d10ba2f3f
LicenseTypes	Base license consumed

Resultado de la regla REDIRECT

ISE | Client Report

Identity Services Engine

Overview

Event	5236 Authorize-Only succeeded
Username	luisgzm
Endpoint Id	E8:4E:06:5D:40:B4
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default
Authorization Policy	Default >> CWA_Luis_Accept
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2023-07-18 00:27:04.599
Received Timestamp	2023-07-18 00:27:04.599
Policy Server	ISE2-luisgzm
Event	5236 Authorize-Only succeeded
Username	luisgzm
User Type	GuestUser
Endpoint Id	E8:4E:06:5D:40:B4
Calling Station Id	e8-4e-06-5d-40-b4
Endpoint Profile	Windows10-Workstation
IPv4 Address	172.16.49.5
Authentication Identity Store	Internal Users

Steps

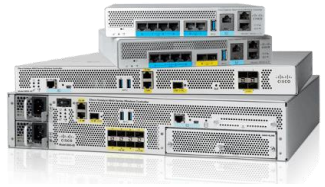
11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
24209	Looking up Endpoint in Internal Endpoints IDStore - luisgzm
24211	Found Endpoint in Internal Endpoints IDStore
15048	Queried PIP - EndPoints.LogicalProfile
15016	Selected Authorization Profile - PermitAccess
11002	Returned RADIUS Access-Accept

Resultado de la regla PERMIT

Result

User-Name	luisgzm
Class	CACS:CD3110AC000001916663195D:ISE2-luisgzm/472937644/201
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base license consumed

C9800 | RadioActive Trace (RA)



#debug platform condition feature wireless mac e84e.065d.40b4

Logging display requested on 2023/07/18 12:16:14 (CST) for Hostname: [9800_LAB_], Model: [C9800-CL-K9], Version: [17.09.03], SN: [XXXX], MD_SN: [XXXXXX]

2023/07/18 12:14:51.421358724 {wncd_x_R0-0}{1}: [client-orch-sm] [14945]: (note): MAC: e84e.065d.40b4 **Association received**. BSSID a4b2.3902.de2c, WLAN L-9800_LAB__CWA, Slot 1 AP a4b2.3902.de20, AP-9130AXI-CALO-

2023/07/18 12:14:51.421635365 {wncd_x_R0-0}{1}: [client-orch-state] [14945]: (note): MAC: e84e.065d.40b4 Client state transition: S_CO_INIT -> S_CO_ASSOCIATING

2023/07/18 12:14:51.422024137 {wncd_x_R0-0}{1}: [client-orch-state] [14945]: (note): MAC: e84e.065d.40b4 Client state transition: S_CO_ASSOCIATING **->** S_CO_MACAUTH_IN_PROGRESS

2023/07/18 12:14:51.422117801 {wncd_x_R0-0}{1}: [client-auth] [14945]: (note): MAC: e84e.065d.40b4 **MAB Authentication initiated**. Policy VLAN 2649, **AAA override = 1**, **NAC = 1**

2023/07/18 12:14:51.423940184 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [14945]: (note): Authentication Success. Resolved Policy bitmap:11 for client e84e.065d.40b4

2023/07/18 12:14:51.562239153 {wncd_x_R0-0}{1}: [client-auth] [14945]: (note): MAC: e84e.065d.40b4 **MAB Authentication success**.

2023/07/18 12:14:51.562410382 {wncd_x_R0-0}{1}: [client-orch-state] [14945]: (note): MAC: e84e.065d.40b4 Client state transition: S_CO_MACAUTH_IN_PROGRESS -> S_CO_ASSOCIATING

2023/07/18 12:14:51.562603690 {wncd_x_R0-0}{1}: [dot11] [14945]: (note): MAC: e84e.065d.40b4 Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False Fast roam = False

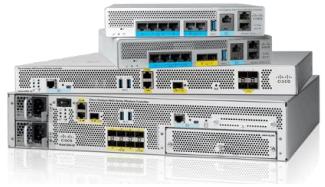
2023/07/18 12:14:51.562829083 {wncd_x_R0-0}{1}: [client-orch-state] [14945]: (note): MAC: e84e.065d.40b4 Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS

2023/07/18 12:14:51.562888833 {wncd_x_R0-0}{1}: [client-auth] [14945]: (note): MAC: e84e.065d.40b4 **L2 WEBAUTH Authentication Successful**

2023/07/18 12:14:51.562960260 {wncd_x_R0-0}{1}: [client-orch-sm] [14945]: (note): MAC: e84e.065d.40b4 Mobility discovery triggered. Client mode: Local

2023/07/18 12:14:51.562962490 {wncd_x_R0-0}{1}: [client-orch-state] [14945]: (note): MAC: e84e.065d.40b4 Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS

C9800 | RadioActive Trace (RA)



Continuacion...

2023/07/18 12:14:51.564985606 {wncd_x_R0-0}{1}: [mm-client] [14945]: (note): MAC: e84e.065d.40b4 Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IFID: 0xa0000001, Client Role: Local PoA: 0x9000000c PoP: 0x0

2023/07/18 12:14:51.565332545 {wncd_x_R0-0}{1}: [client-auth] [14945]: (note): MAC: e84e.065d.40b4 ADD MOBILE sent. Client state flags: 0x72 BSSID: MAC: a4b2.3902.de2c capwap IFID: 0x9000000c, Add mobiles sent: 1

2023/07/18 12:14:51.565365463 {wncd_x_R0-0}{1}: [client-orch-state] [14945]: (note): MAC: e84e.065d.40b4 Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS

2023/07/18 12:14:51.565486353 {wncd_x_R0-0}{1}: [dot11] [14945]: (note): MAC: e84e.065d.40b4 Client datapath entry params - ssid:L-9800_LAB__CWA,slot_id:1 bssid ifid: 0x0, radio_ifid: 0x90000003, wlan_ifid: 0xf0400004

2023/07/18 12:14:51.566197129 {wncd_x_R0-0}{1}: [dpath_svc] [14945]: (note): MAC: e84e.065d.40b4 Client datapath entry created for ifid 0xa0000001

2023/07/18 12:14:51.566831397 {wncd_x_R0-0}{1}: [client-orch-state] [14945]: (note): MAC: e84e.065d.40b4 Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

2023/07/18 12:14:51.636016648 {wncd_x_R0-0}{1}: [client-iplearn] [14945]: (note): MAC: e84e.065d.40b4 Client IP learn successful. Method: DHCP IP: 172.16.49.5

2023/07/18 12:14:51.636716513 {wncd_x_R0-0}{1}: [client-orch-state] [14945]: (note): MAC: e84e.065d.40b4 Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS

C9800 | RadioActive Trace (RA)

Continuacion...

2023/07/18 12:14:51.636768266 {wncd_x_R0-0}{1}: [client-auth] [14945]: (note): MAC: e84e.065d.40b4 L3 Authentication initiated. CWA

2023/07/18 12:15:21.337366555 {wncd_x_R0-0}{1}: [client-auth] [14945]: (note): MAC: e84e.065d.40b4 L3 Authentication Successful. ACL:[]

2023/07/18 12:15:21.337823656 {wncd_x_R0-0}{1}: [client-auth] [14945]: (note): MAC: e84e.065d.40b4 ADD MOBILE sent. Client state flags: 0x78 BSSID: MAC: a4b2.3902.de2c capwap IFID: 0x9000000c, Add mobiles sent: 1

2023/07/18 12:15:21.338017738 {wncd_x_R0-0}{1}: [errmsg] [14945]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: Username entry (luisgzm) joined with ssid (L-9800_LAB__CWA) for device with MAC: e84e.065d.40b4

2023/07/18 12:15:21.338299010 {wncd_x_R0-0}{1}: [client-orch-state] [14945]: (note): MAC: e84e.065d.40b4 Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Perspectiva del Controlador | MAB

No.	Time	Source	Destination	Protocol	Destinat	Length	Differentiated Ser	Sequence	ID	Identification	Info
106	12:14:51.423974	172.16.49.205	172.16.48.196	RADIUS	1812	483	Default		2649	0x831b (33563)	Access-Request id=15
107	12:14:51.557969	172.16.48.196	172.16.49.205	RADIUS	61605	627	Default			0x6d28 (27944)	Access-Accept id=15

```
> Frame 106: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits)
> Ethernet II, Src: Cisco_ed:d8:ff (00:1e:bd:ed:d8:ff), Dst: Cisco_9f:f0:31 (00:00:0c:9f:f0:31)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2649
> Internet Protocol Version 4, Src: 172.16.49.205, Dst: 172.16.48.196
> User Datagram Protocol, Src Port: 61605, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0xf (15)
    Length: 437
    Authenticator: 2961e80150e8ca743ecdb6d1851b920a
    [The response to this request is in frame 107]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=14 val=e84e065d40b4
    > AVP: t=User-Password(2) l=18 val=Decrypted: e84e065d40b4
    > AVP: t=Service-Type(6) l=6 val=Call-Check(10)
    > AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
    > AVP: t=Framed-MTU(12) l=6 val=1485
    > AVP: t=Message-Authenticator(80) l=18 val=d59ec179d009c5481bbf04ba259a822d
    > AVP: t=EAP-Key-Name(102) l=2 val=
    > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=18 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
    > AVP: t=NAS-IP-Address(4) l=6 val=172.16.49.205
    > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
    > AVP: t=NAS-Port(5) l=6 val=264911
    > AVP: t=Vendor-Specific(26) l=46 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=48 vnd=ciscoSystems(9)
    > AVP: t=Called-Station-Id(30) l=42 val=a4-b2-39-02-de-20:L-9800_LAB_luisgzm_CWA
    > AVP: t=Calling-Station-Id(31) l=19 val=e8-4e-06-5d-40-b4
    > AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
    > AVP: t=NAS-Identifier(32) l=18 val=9800_LAB_luisgzm
```

WLC Uplink Capture

Perspectiva del Controlador | MAB

No.	Time	Source	Destination	Protocol	Destinat	Length	Differentiated Ser	Sequence	ID	Identification	Info
106	12:14:51.423974	172.16.49.205	172.16.48.196	RADIUS	1812	483	Default		2649	0x831b (33563)	Access-Request id=15
107	12:14:51.557969	172.16.48.196	172.16.49.205	RADIUS	61605	627	Default			0x6d28 (27944)	Access-Accept id=15

```
> Frame 107: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits)
> Ethernet II, Src: Cisco_3f:80:f1 (78:da:6e:3f:80:f1), Dst: Cisco_ed:d8:ff (00:1e:bd:ed:d8:ff)
> Internet Protocol Version 4, Src: 172.16.48.196, Dst: 172.16.49.205
> User Datagram Protocol, Src Port: 1812, Dst Port: 61605
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0xf (15)
    Length: 585
    Authenticator: b67779bfbfa8083cb3f53c1436eb1db6
    [This is a response to a request in frame 106]
    [Time from request: 0.133995000 seconds]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=19 val=E8-4E-06-5D-40-B4
    > AVP: t=Class(25) l=58 val=434143533a434433313130414330303030303139333641333537343941 3a495345322d6c…
    > AVP: t=Message-Authenticator(80) l=18 val=248bfe0858ef87d275d992399933dbfa
    v AVP: t=Vendor-Specific(26) l=200 vnd=ciscoSystems(9)
        Type: 26
        Length: 200
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=194 val=url-redirect=https://ISE2-luisgzm.local.com:8443/portal/gateway?sessionId=CD3110AC000001936A35749A&portal=f0ae43f0-7159-11e7-a355-005056aba474&action=cwa&token=e6222116abc0230f08473a5ea55bb37e
    v AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(9)
        Type: 26
        Length: 37
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=31 val=url-redirect-acl=CWA_REDIRECT
    v AVP: t=Vendor-Specific(26) l=191 vnd=ciscoSystems(9)
        Type: 26
        Length: 191
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=185 val=url-redirect=https://172.16.48.196:8443/portal/gateway?sessionId=CD3110AC000001936A35749A&portal=f0ae43f0-7159-11e7-a355-005056aba474&action=cwa&token=16d36db2622b5c322898e8d4f8836a45
    v AVP: t=Vendor-Specific(26) l=42 vnd=ciscoSystems(9)
        Type: 26
        Length: 42
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=36 val=profile-name=Windows10-Workstation
```

Windows Wireless NIC Capture

Perspectiva del Cliente | DHCP

20	11:59:53.823931	0.0.0.0	255.255.255.255	DHCP	67	352	Default	0x9a1a (39450)	DHCP Request	– Transaction ID 0x793e0916
21	11:59:53.829268	172.16.49.253	255.255.255.255	DHCP	68	342	Default	0x61f9 (25081)	DHCP ACK	– Transaction ID 0x793e0916

```
> Frame 21: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{770571B7-5A9F-4B04-99FF-84AEE5FD0BF3}, id 0
> Ethernet II, Src: Cisco_46:2f:61 (88:5a:92:46:2f:61), Dst: EdupInte_5d:40:b4 (e8:4e:06:5d:40:b4)
> Internet Protocol Version 4, Src: 172.16.49.253, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x793e0916
    Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 172.16.49.5
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: EdupInte_5d:40:b4 (e8:4e:06:5d:40:b4)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (54) DHCP Server Identifier (172.16.49.253)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (43) Vendor-Specific Information
  > Option: (255) End
    Padding: 000000000000
```

Perspectiva del Cliente | DNS Resolution

48	11:59:54.633214	172.16.49.5	72.163.47.11	DNS	53	83	Default	0x9c25 (39973)	Standard query 0x0969 A www.msftconnecttest.com
53	11:59:54.711892	72.163.47.11	172.16.49.5	DNS	53166	233	Default	0x42ed (17133)	Standard query response 0x0969 A www.msftconnec

```
> Frame 48: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{770571B7-5A9F-4B04-99FF-84AEE5FD0BF3}, id 0
> Ethernet II, Src: EdupInte_5d:40:b4 (e8:4e:06:5d:40:b4), Dst: Cisco_9f:f0:31 (00:00:0c:9f:f0:31)
> Internet Protocol Version 4, Src: 172.16.49.5, Dst: 72.163.47.11
> User Datagram Protocol, Src Port: 53166, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0969
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.msftconnecttest.com: type A, class IN
    [Response In: 53]
```

48	11:59:54.633214	172.16.49.5	72.163.47.11	DNS	53	83	Default	0x9c25 (39973)	Standard query 0x0969 A www.msftconnecttest.com
53	11:59:54.711892	72.163.47.11	172.16.49.5	DNS	53166	233	Default	0x42ed (17133)	Standard query response 0x0969 A www.msftconnect

```
> Frame 53: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface \Device\NPF_{770571B7-5A9F-4B04-99FF-84AEE5FD0BF3}, id 0
> Ethernet II, Src: Cisco_3f:80:f1 (78:da:6e:3f:80:f1), Dst: EdupInte_5d:40:b4 (e8:4e:06:5d:40:b4)
> Internet Protocol Version 4, Src: 72.163.47.11, Dst: 172.16.49.5
> User Datagram Protocol, Src Port: 53, Dst Port: 53166
v Domain Name System (response)
    Transaction ID: 0x0969
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.msftconnecttest.com: type A, class IN
  v Answers
    > www.msftconnecttest.com: type CNAME, class IN, cname ncsi-geo.trafficmanager.net
    > ncsi-geo.trafficmanager.net: type CNAME, class IN, cname www.msftncsi.com.edgesuite.net
    > www.msftncsi.com.edgesuite.net: type CNAME, class IN, cname a1961.g2.akamai.net
    > a1961.g2.akamai.net: type A, class IN, addr 104.117.244.33
    > a1961.g2.akamai.net: type A, class IN, addr 104.117.244.11
    [Request In: 48]
    [Time: 0.078678000 seconds]
```

Windows Wireless NIC Capture

Perspectiva del Cliente | TCP Hijack

54	11:59:54.712872	172.16.49.5	104.117.244.33	TCP	66	Default	0	0x764b (30283)	49769 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
55	11:59:54.717491	104.117.244.33	172.16.49.5	TCP	66	Default	0	0x0000 (0)	80 → 49769 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1250 SACK_PERM WS=128
56	11:59:54.717563	172.16.49.5	104.117.244.33	TCP	54	Default	1	0x764c (30284)	49769 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0

```
> Frame 55: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{770571B7-5A9F-4B04-99FF-84AEE5FD0BF3}, id 0
v Ethernet II, Src: Cisco_9f:f0:31 (00:00:0c:9f:f0:31), Dst: EdupInte_5d:40:b4 (e8:4e:06:5d:40:b4)
  > Destination: EdupInte_5d:40:b4 (e8:4e:06:5d:40:b4)
  > Source: Cisco_9f:f0:31 (00:00:0c:9f:f0:31)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 104.117.244.33, Dst: 172.16.49.5
v Transmission Control Protocol, Src Port: 80, Dst Port: 49769, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 49769
    [Stream index: 1]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1829000279
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3319228761
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x87ef [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
  > [Timestamps]
  > [SEQ/ACK analysis]
```

Windows Wireless NIC Capture

Perspectiva del Cliente | HTTP GET | Regla Redirect

No.	Time	Source	Destination	Protocol	Destinal	Length	Differentiated Ser	Sequence	ID	Identification	Info
57	11:59:54.717931	172.16.49.5	104.117.244.33	HTTP		165	Default	1		0x764d (30285)	GET /connecttest.txt HTTP/1.1
59	11:59:54.721455	104.117.244.33	172.16.49.5	HTTP		910	Default	1		0x9c75 (40053)	HTTP/1.1 200 OK (text/html)

```
> Frame 57: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{770571B7-5A9F-4B04-99FF-84AEE5FD0BF3}, id 0
> Ethernet II, Src: EdupInte_5d:40:b4 (e8:4e:06:5d:40:b4), Dst: Cisco_9f:f0:31 (00:00:0c:9f:f0:31)
> Internet Protocol Version 4, Src: 172.16.49.5, Dst: 104.117.244.33
> Transmission Control Protocol, Src Port: 49769, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
v Hypertext Transfer Protocol
  > GET /connecttest.txt HTTP/1.1\r\n
    Connection: Close\r\n
    User-Agent: Microsoft NCSI\r\n
    Host: www.msftconnecttest.com\r\n
    \r\n
    [Full request URI: http://www.msftconnecttest.com/connecttest.txt]
    [HTTP request 1/1]
    [Response in frame: 59]
```

Windows Wireless NIC Capture

Perspectiva del Cliente | HTTP Redirection

No.	Time	Source	Destination	Protocol	Destinat	Length	Differentiated Ser	Sequence	ID	Identification	Info
57	11:59:54.717931	172.16.49.5	104.117.244.33	HTTP		165	Default	1		0x764d (30285)	GET /connecttest.txt HTTP/1.1
59	11:59:54.721455	104.117.244.33	172.16.49.5	HTTP		910	Default	1		0x9c75 (40053)	HTTP/1.1 200 OK (text/html)

```
> Frame 59: 910 bytes on wire (7280 bits), 910 bytes captured (7280 bits) on interface \Device\NPF_{770571B7-5A9F-4B04-99FF-84AEE5FD0BF3}, id 0
> Ethernet II, Src: Cisco_9f:f0:31 (00:00:0c:9f:f0:31), Dst: EdupInte_5d:40:b4 (e8:4e:06:5d:40:b4)
> Internet Protocol Version 4, Src: 104.117.244.33, Dst: 172.16.49.5
> Transmission Control Protocol, Src Port: 80, Dst Port: 49769, Seq: 1, Ack: 112, Len: 856
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    [truncated]Location: https://172.16.48.196:8443/portal/gateway?sessionId=CD3110AC000001936A35749A&portal=f0ae43f0-7159-11e7-a355-005056aba474&action=cwa&token=16d36db2622b5c322898e8d4f8836a45&redirect=http://www.msftconnecttest.com/conne
    Content-Type: text/html\r\n
  > Content-Length: 553\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.003524000 seconds]
    [Request in frame: 57]
    [Request URI: http://www.msftconnecttest.com/connecttest.txt]
    File Data: 553 bytes
v Line-based text data: text/html (9 lines)
    <HTML><meta name="viewport" content="width=device-width, initial-scale=1">\n
    <HEAD>\n
    <TITLE> Web Authentication Redirect</TITLE>\n
    <META http-equiv="Cache-control" content="no-cache">\n
    <META http-equiv="Pragma" content="no-cache">\n
    <META http-equiv="Expires" content="-1">\n
    [truncated]<META http-equiv="refresh" content="1; URL=https://172.16.48.196:8443/portal/gateway?sessionId=CD3110AC000001936A35749A&portal=f0ae43f0-7159-11e7-a355-005056aba474&action=cwa&token=16d36db2622b5c322898e8d4f8836a45&redirect=htt
    </HEAD>\n
```

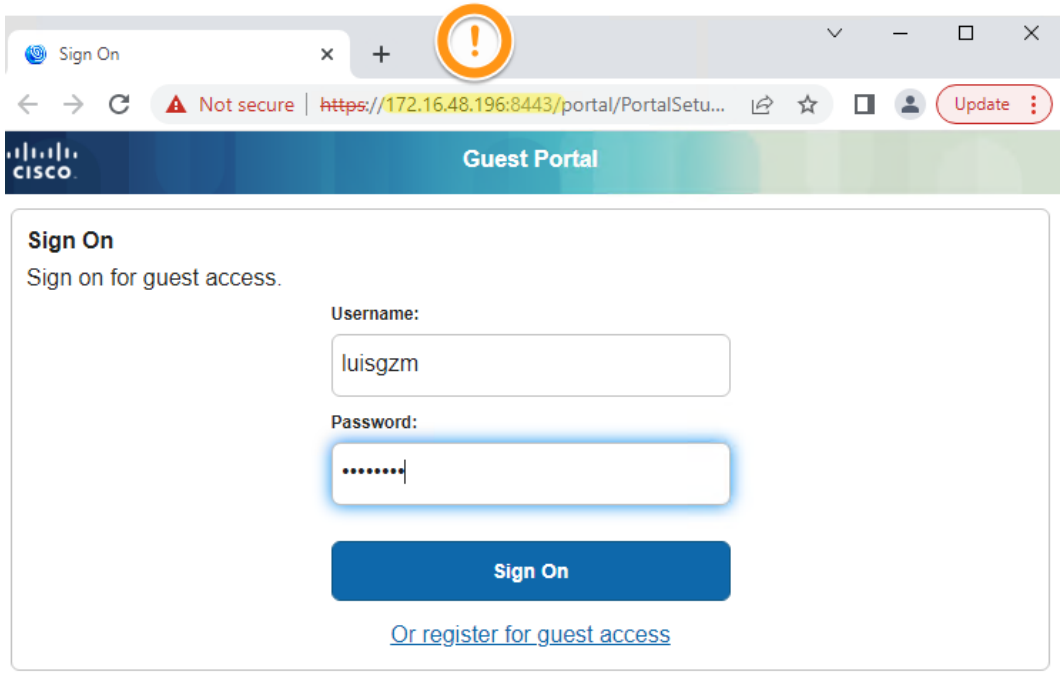
Windows Wireless NIC Capture

Perspectiva del Cliente | TCP and TLS

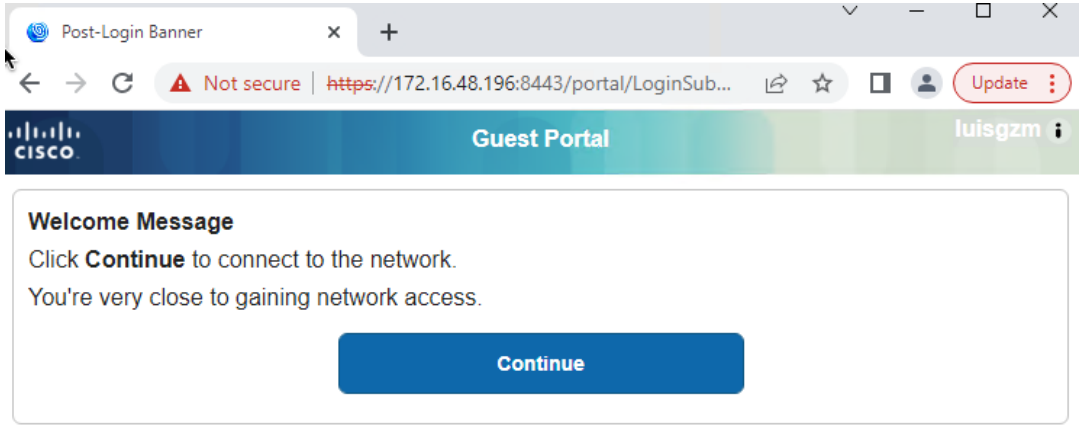
No.	Time	Source	Destination	Protocol	Destinat	Length	Differentiated Ser	Sequence	ID	Identification	Info
158	12:00:03.220597	172.16.49.5	172.16.48.196	TCP		66	Default	0		0x70a4 (28836)	49798 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
159	12:00:03.220891	172.16.49.5	172.16.48.196	TCP		66	Default	0		0x70a5 (28837)	49799 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
160	12:00:03.225766	172.16.48.196	172.16.49.5	TCP		66	Default	0		0x0000 (0)	8443 → 49798 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128
161	12:00:03.225766	172.16.48.196	172.16.49.5	TCP		66	Default	0		0x0000 (0)	8443 → 49799 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128
162	12:00:03.225820	172.16.49.5	172.16.48.196	TCP		54	Default	1		0x70a6 (28838)	49798 → 8443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
163	12:00:03.225869	172.16.49.5	172.16.48.196	TCP		54	Default	1		0x70a7 (28839)	49799 → 8443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
164	12:00:03.237186	172.16.49.5	172.16.48.196	TLSv1.2		571	Default	1		0x70a8 (28840)	Client Hello
165	12:00:03.240264	172.16.49.5	172.16.48.196	TLSv1.2		571	Default	1		0x70a9 (28841)	Client Hello
166	12:00:03.242580	172.16.48.196	172.16.49.5	TCP		54	Default	1		0x6f20 (28448)	8443 → 49799 [ACK] Seq=1 Ack=518 Win=30336 Len=0
167	12:00:03.244719	172.16.48.196	172.16.49.5	TCP		54	Default	1		0x7ceb (31979)	8443 → 49798 [ACK] Seq=1 Ack=518 Win=30336 Len=0
168	12:00:03.247278	172.16.48.196	172.16.49.5	TCP		1304	Default	1		0x6f21 (28449)	8443 → 49799 [ACK] Seq=1 Ack=518 Win=30336 Len=1250 [TCP segment of a reassembl
169	12:00:03.247278	172.16.48.196	172.16.49.5	TLSv1.2		71	Default	1251		0x6f22 (28450)	Server Hello, Certificate, Server Key Exchange, Server Hello Done
170	12:00:03.247303	172.16.49.5	172.16.48.196	TCP		54	Default	518		0x70aa (28842)	49799 → 8443 [ACK] Seq=518 Ack=1268 Win=66048 Len=0
171	12:00:03.250645	172.16.48.196	172.16.49.5	TCP		1304	Default	1		0x7cec (31980)	8443 → 49798 [ACK] Seq=1 Ack=518 Win=30336 Len=1250 [TCP segment of a reassembl
172	12:00:03.250645	172.16.48.196	172.16.49.5	TLSv1.2		71	Default	1251		0x7ced (31981)	Server Hello, Certificate, Server Key Exchange, Server Hello Done

```
> Frame 158: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{770571B7-5A9F-4B04-99FF-84AEE5FD0BF3}, id 0
> Ethernet II, Src: EdupInte_5d:40:b4 (e8:4e:06:5d:40:b4), Dst: Cisco_9f:f0:31 (00:00:0c:9f:f0:31)
> Internet Protocol Version 4, Src: 172.16.49.5, Dst: 172.16.48.196
> Transmission Control Protocol, Src Port: 49798, Dst Port: 8443, Seq: 0, Len: 0
```

Perspectiva del Cliente | Navegador



Authentication Portal



WLC Uplink Capture

Perspectiva del Controlador | RADIUS CoA Request

No.	Time	Source	Destination	Protocol	Destinat	Length	Differentiated Ser	Sequence	ID	Identification	Info
1569	12:15:21.313979	172.16.48.196	172.16.49.205	RADIUS	1700	244	Default			0x7904 (30980)	CoA-Request id=2
1571	12:15:21.314970	172.16.49.205	172.16.48.196	RADIUS	35403	115	Default		2649	0xeb25 (60197)	CoA-ACK id=2

```
> Frame 1569: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
> Ethernet II, Src: Cisco_3f:80:f1 (78:da:6e:3f:80:f1), Dst: Cisco_ed:d8:ff (00:1e:bd:ed:d8:ff)
> Internet Protocol Version 4, Src: 172.16.48.196, Dst: 172.16.49.205
> User Datagram Protocol, Src Port: 35403, Dst Port: 1700
v RADIUS Protocol
    Code: CoA-Request (43)
    Packet identifier: 0x2 (2)
    Length: 202
    Authenticator: 3b61a9d5a55afdfd82fce798a58e345d
    [The response to this request is in frame 1571]
  v Attribute Value Pairs
    > AVP: t=NAS-IP-Address(4) l=6 val=172.16.49.205
    > AVP: t=Calling-Station-Id(31) l=19 val=e8-4e-06-5d-40-b4
    > AVP: t=Event-Timestamp(55) l=6 val=Jul 18, 2023 12:15:21.000000000 CST
    > AVP: t=Message-Authenticator(80) l=18 val=41cd1f6978b43fd8e07d2eaa4f99a69e
    v AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
        Type: 26
        Length: 41
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=35 val=subscriber:command=reauthenticate
    v AVP: t=Vendor-Specific(26) l=43 vnd=ciscoSystems(9)
        Type: 26
        Length: 43
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=37 val=subscriber:reauthenticate-type=last
    v AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
        Type: 26
        Length: 49
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=43 val=audit-session-id=CD3110AC000001936A35749A
```

WLC Uplink Capture

Perspectiva del Controlador | RADIUS CoA Response

No.	Time	Source	Destination	Protocol	Destinat	Length	Differentiated Ser	Sequence	ID	Identification	Info
1569	12:15:21.313979	172.16.48.196	172.16.49.205	RADIUS	1700	244	Default			0x7904 (30980)	CoA-Request id=2
1571	12:15:21.314970	172.16.49.205	172.16.48.196	RADIUS	35403	115	Default		2649	0xeb25 (60197)	CoA-ACK id=2

```
> Frame 1571: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
> Ethernet II, Src: Cisco_ed:d8:ff (00:1e:bd:ed:d8:ff), Dst: Cisco_9f:f0:31 (00:00:0c:9f:f0:31)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2649
> Internet Protocol Version 4, Src: 172.16.49.205, Dst: 172.16.48.196
> User Datagram Protocol, Src Port: 1700, Dst Port: 35403
v RADIUS Protocol
    Code: CoA-ACK (44)
    Packet identifier: 0x2 (2)
    Length: 69
    Authenticator: 3ce7eaaeaa7f22fdd4f6c024df569357
    [This is a response to a request in frame 1569]
    [Time from request: 0.000991000 seconds]
  v Attribute Value Pairs
    v AVP: t=Vendor-Specific(26) l=9 vnd=ciscoSystems(9)
        Type: 26
        Length: 9
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-Command-Code(252) l=3 val=2
    > AVP: t=Calling-Station-Id(31) l=16 val=e84e.065d.40b4
    > AVP: t=Error-Cause(101) l=6 val=Unknown(200)
    > AVP: t=Message-Authenticator(80) l=18 val=c80e9f12f871636486396d735337feb4
```

WLC Uplink Capture

Perspectiva del Controlador | Regla Permit

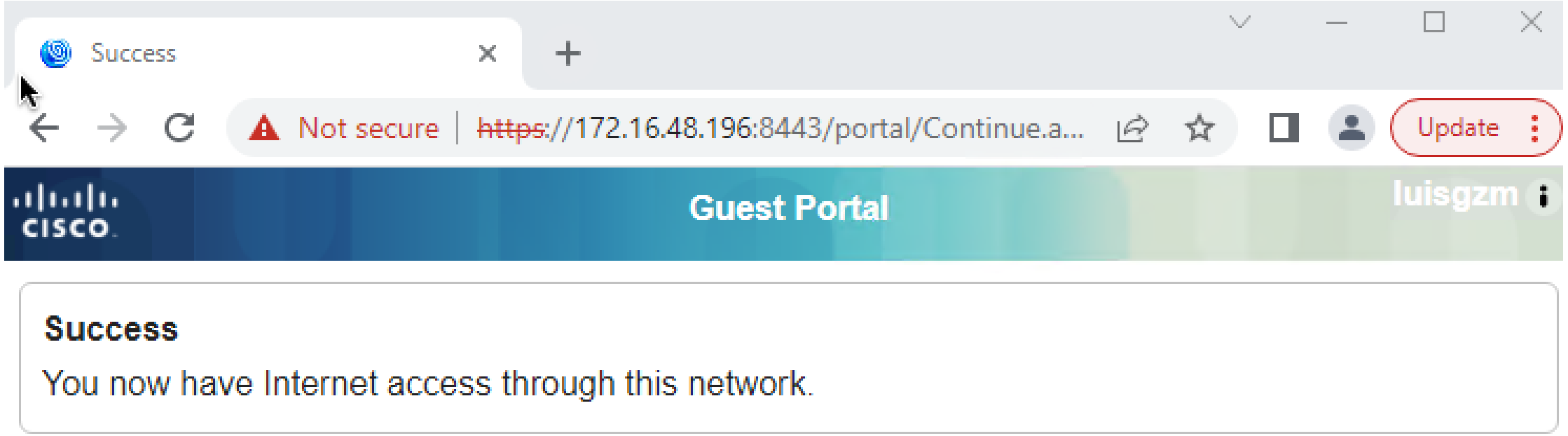
```
1570 12:15:21.314970 172.16.49.205  172.16.48.196  RADIUS  1812  489  Default  2649 0xeb24 (60196)  Access-Request id=23
1572 12:15:21.334974 172.16.48.196  172.16.49.205  RADIUS  61605 189  Default       0x791a (31002)  Access-Accept id=23

> Frame 1570: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Cisco_ed:d8:ff (00:1e:bd:ed:d8:ff), Dst: Cisco_9f:f0:31 (00:00:0c:9f:f0:31)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2649
> Internet Protocol Version 4, Src: 172.16.49.205, Dst: 172.16.48.196
> User Datagram Protocol, Src Port: 61605, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x17 (23)
    Length: 443
    Authenticator: fe1298dca40aca0589e58c1ef5c5df1e
    [The response to this request is in frame 1572]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=14 val=e84e065d40b4
    > AVP: t=User-Password(2) l=18 val=Decrypted: e84e065d40b4
    > AVP: t=Service-Type(6) l=6 val=Call-Check(10)
    > AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
    > AVP: t=Framed-MTU(12) l=6 val=1485
    > AVP: t=Message-Authenticator(80) l=18 val=f81e02724d9202513d511c0a08dc34e3
    > AVP: t=EAP-Key-Name(102) l=2 val=
    v AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
        Type: 26
        Length: 49
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=43 val=audit-session-id=CD3110AC000001936A35749A
    > AVP: t=Vendor-Specific(26) l=18 vnd=ciscoSystems(9)
    > AVP: t=Framed-IP-Address(8) l=6 val=172.16.49.5
    > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
    > AVP: t=NAS-IP-Address(4) l=6 val=172.16.49.205
    > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
    > AVP: t=NAS-Port(5) l=6 val=264911
    > AVP: t=Vendor-Specific(26) l=46 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=48 vnd=ciscoSystems(9)
    > AVP: t=Called-Station-Id(30) l=42 val=a4-b2-39-02-de-20:L-9800_LAB_luisgzm_CWA
    > AVP: t=Calling-Station-Id(31) l=19 val=e8-4e-06-5d-40-b4
    > AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
    > AVP: t=NAS-Identifier(32) l=18 val=9800_LAB_luisgzm
```

Perspectiva del Controlador | 2do Access Accept

1570	12:15:21.314970	172.16.49.205	172.16.48.196	RADIUS	1812	489	Default	2649	0xeb24 (60196)	Access-Request id=23
1572	12:15:21.334974	172.16.48.196	172.16.49.205	RADIUS	61605	189	Default		0x791a (31002)	Access-Accept id=23

```
> Frame 1572: 189 bytes on wire (1512 bits), 189 bytes captured (1512 bits)
> Ethernet II, Src: Cisco_3f:80:f1 (78:da:6e:3f:80:f1), Dst: Cisco_ed:d8:ff (00:1e:bd:ed:d8:ff)
> Internet Protocol Version 4, Src: 172.16.48.196, Dst: 172.16.49.205
> User Datagram Protocol, Src Port: 1812, Dst Port: 61605
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x17 (23)
    Length: 147
    Authenticator: 756fdfc195e7ace3af387a751ad83b56
    [This is a response to a request in frame 1570]
    [Time from request: 0.020004000 seconds]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=9 val=luisgzm
    > AVP: t=Class(25) l=58 val=434143533a434433313130414330303030303139333641333537343941 3a495345322d6c…
    > AVP: t=Message-Authenticator(80) l=18 val=e008ae335aabd054a7d0bad92d3d125d
    > AVP: t=Vendor-Specific(26) l=42 vnd=ciscoSystems(9)
```

Perspectiva del Cliente | End User Perspective



Información Adicional sobre ISE & Webauth

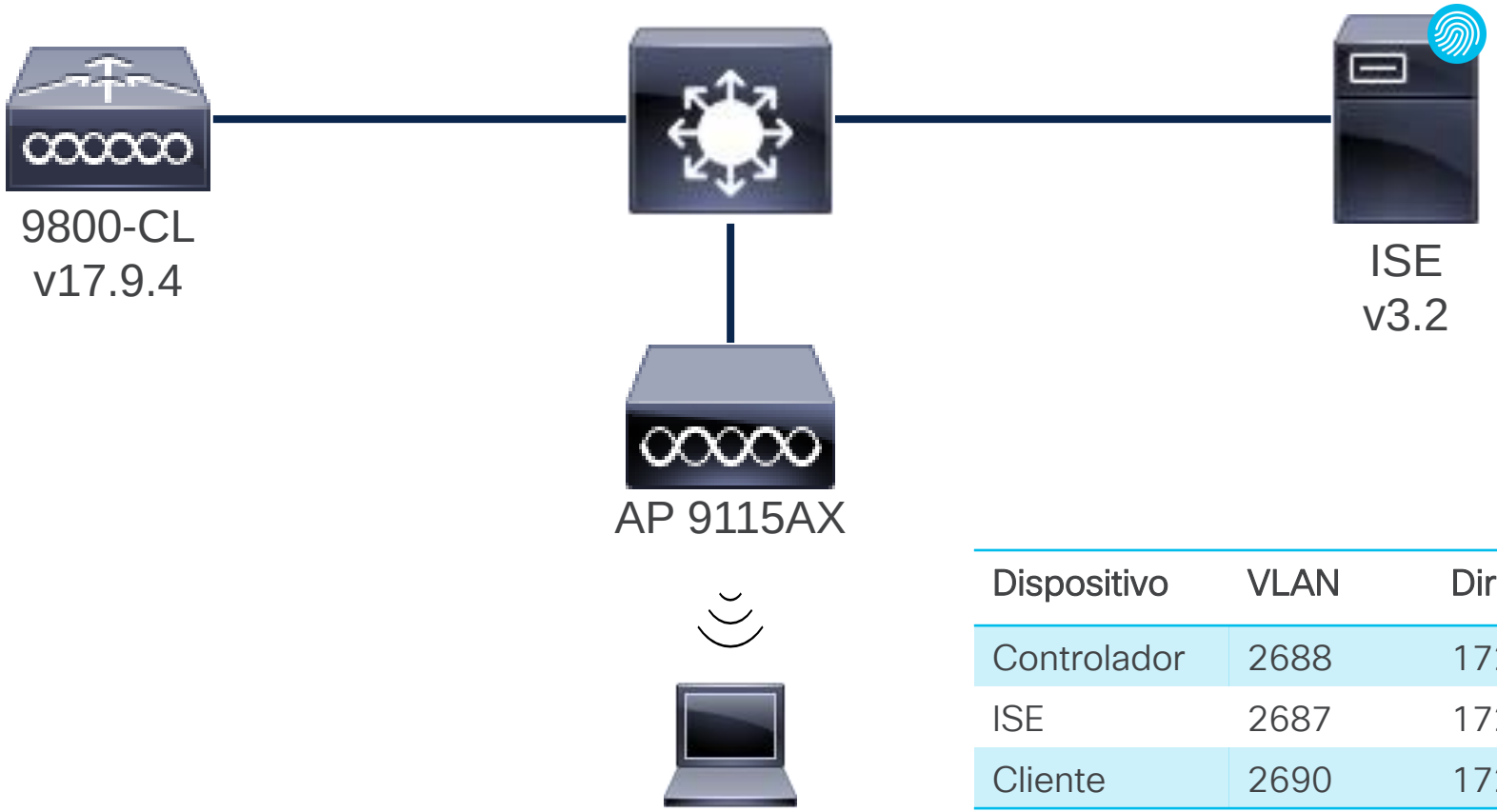
- ISE Guest & Web Authentication

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

6. Demostración

Introducción
Proceso de autenticación web
CWA en controladores Catalyst serie 9800
Túnel de movilidad: Foreign-Anchor
Diagnóstico y resolución de problemas
Demo

Diagrama de Red



Dispositivo	VLAN	Dirección
Controlador	2688	172.16.95.90
ISE	2687	172.16.94.20
Cliente	2690	172.16.97.0/24

¡Manos a la Obra! CWA

Antes

- Autenticación Web tradicional (LWA) no es Escalable
- Típicamente Usuario / Password para Guest compartido
- Red de Guest poco aisalda de la Red Coorporativa
- Portal Web poco personalizable

Después

- ✓ CWA te permite tener un solo punto de administración
- ✓ ISE puede ser configurado para consultar la base de datos existentes (como Active Directory)
- ✓ Mejor experiencia para usuario final: habilidad de crear usuarios temporales (Autoservicio)
- ✓ CWA con Foreign-Anchor evita brechas de seguridad aislando el tráfico Guest en la DMZ
- ✓ ISE puede crear flujos más complejos (BYOD, Posture)
- ✓ CWA puede ser utilizado en la red corporativa como complemento a 802.1x o para usos específicos (ejemplo: acceso a internet de usuarios corporativos)
- ✓ Diferentes Portales y opciones de personalización

Cisco TAC recomienda

Cisco RADKIT

Cisco RADKit permite un servicio de soporte ágil con un mínimo de sobrecarga para los usuarios durante troubleshooting

Wireless TAC-Ready

¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar ¡Nuestros expertos aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) antes del viernes 13 de octubre de 2023

https://bit.ly/CLama-oct23

Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!

Al término de esta sesión, se abrirá una encuesta en su navegador.

Nuestras Redes Sociales

LinkedIn

Cisco Community

Twitter

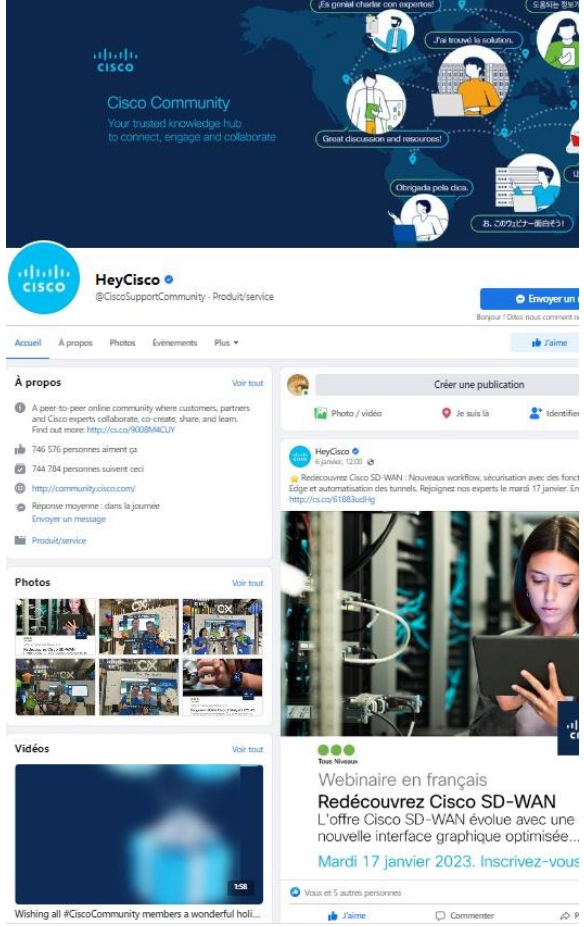
@CiscoCommunity

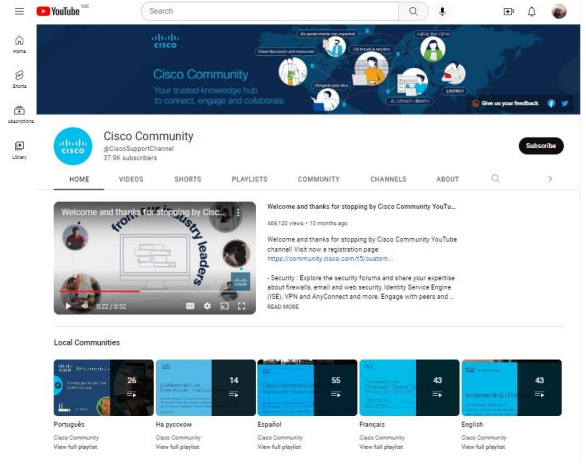
YouTube

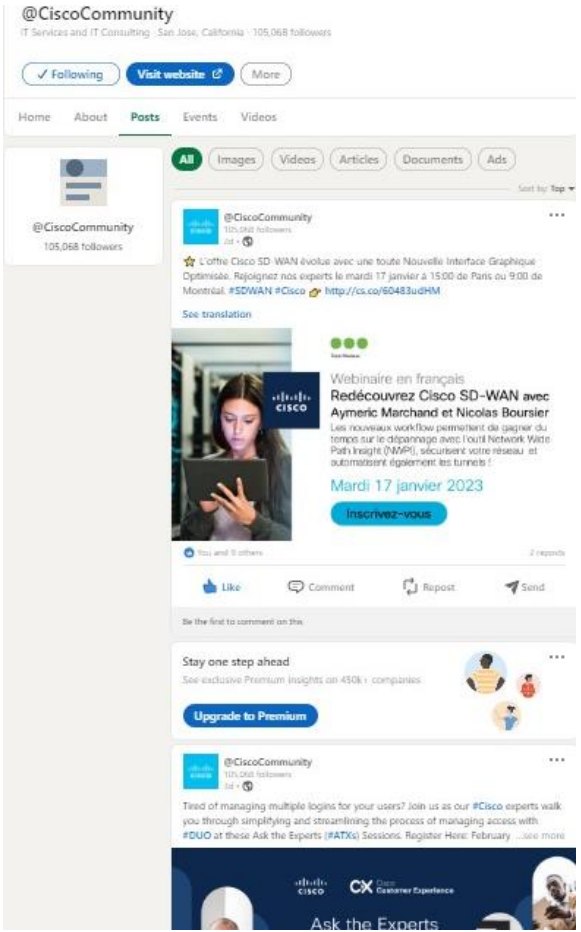
CiscoSupportChannel

Facebook

CiscoSupportCommunity







CISCO

The bridge to possible