Configuración de FlexConnect OEAP con tunelización dividida

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Overview Hechos importantes Configurar Diagrama de la red Configuraciones configuración WLAN Configuración de AP Verificación

Introducción

Este documento describe cómo configurar un punto de acceso interior (AP) como modo de punto de acceso de extensión de oficina (OEAP) de FlexConnect y cómo habilitar la tunelización dividida para que pueda definir qué tráfico debe conmutarse localmente en la oficina doméstica y qué tráfico debe conmutarse centralmente en el controlador de LAN inalámbrica (WLC).

Colaborado por Tiago Antunes, Nicolas Darchis Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Hay configuración en este documento que asume que el WLC ya está configurado en una zona desmilitarizada (DMZ) con traducción de direcciones de red (NAT) habilitada y que el AP puede unirse al WLC desde la oficina principal.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC con la versión AireOS 8.10(130.0) Software.
- AP Wave1: 1700/2700/3700.
- AP Wave2: 1800/2800/3800/4800 y Catalyst serie 9100.

The information in this document was created from the devices in a specific lab environment.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Un OEAP proporciona comunicaciones seguras de un WLC de Cisco a un AP de Cisco en una ubicación remota, para extender la WLAN corporativa a través de Internet a la residencia de un empleado. La experiencia del usuario en la oficina doméstica es exactamente la misma que en la oficina corporativa. El cifrado de seguridad de la capa de transporte del datagrama (DTLS) entre el punto de acceso y el controlador garantiza que todas las comunicaciones tengan el mayor nivel de seguridad. Cualquier punto de acceso interior en modo FlexConnect puede actuar como OEAP.

Hechos importantes

- Los OEAP de Cisco están diseñados para funcionar detrás de un router u otro dispositivo de gateway que utilice NAT. NAT permite que un dispositivo, como un router, actúe como agente entre Internet (pública) y una red personal (privada), lo que permite que un grupo completo de ordenadores se represente mediante una única dirección IP. No hay límite en el número de OEAP de Cisco que puede implementar detrás de un dispositivo NAT.
- Todos los modelos de AP interiores soportados con antena integrada se pueden configurar como OEAP excepto los AP-700I, AP-700W y los AP802 series AP.
- Todos los OEAP deben estar en el mismo grupo AP y ese grupo no debe contener más de 15 LAN inalámbricas. Un controlador con OEAP en un grupo AP publica sólo hasta 15 WLAN a cada OEAP conectado porque reserva una WLAN para el identificador personal del conjunto de servicios (SSID).

Configurar

Diagrama de la red



Configuraciones

configuración WLAN

Paso 1. Cree una WLAN para asignar al grupo AP. No necesita habilitar la opción FlexConnect Local Switching para esta WLAN.

uluulu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS	5 HELP FEEDBACK
WLANs	WLANs > Edit 'FlexOEAP_TEST'	
VLANs	General Security QoS Policy-Mapping Advanced	
Advanced	MBO State	KTS based CAC Policy Enabled
	Off Channel Scanning Defer	Radius Client Profiling
	Scan Defer Priority 0 1 2 3 4 5 6 7	DHCP Profiling
		HTTP Profiling
	Scan Defer Time(msecs) 100	Local Client Profiling
	FlexConnect	DHCP Profiling
	FlexConnect Local Enabled	HTTP Profiling
	Switching 2 Chables	PMIP
	FlexConnect Local Auth 12 Enabled	PMIP Mobility Type
	Learn Client IP Address 2 🖾 Enabled	PMIP NAI Type Hexadecimal ¥
	Vian based Central Enabled	PMIP Profile None V
	Central DHCP Processing Enabled	PMIP Realm
	Override DNS Enabled	Universal AP Admin Support
	NAT-PAT Enabled	Universal AP Admin
	Central Assoc	11v BSS Transition Support

Paso 2. Cree un grupo AP. En la pestaña **WLANs**, elija el WLAN SSID y luego haga clic en **Add** para agregar la WLAN. Vaya a la pestaña **APs** y **Agregar** el OEAP FlexConnect.

iiliiilii cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'
VLANs	General WLANS RF Profile APs 802.11u Location Ports/Module Intelligent Capture
AP Groups	Add New WLAN SSID Interface Group(G) SNMP NAC State WLAN ID WLAN SSID ^{(2)(g)} Interface/Interface Group(G) SNMP NAC State
ululu cisco	10NITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'
VLANS	General WLANS RF Profile APs 802.11u Location Ports/Module Intelligent Capture
 Advanced AP Groups 	APs currently in the Group Remove APs Add APs to the Group Add APs AP Name Ethernet MAC AP Name Group Name AP9120_4C.E77C c4:f7:d5:4c:e7:7c AP3800_E1.3EB8 70:db:98:e1:3e:b8

Después de que el AP se haya asociado con el controlador en el modo FlexConnect, puede configurarlo como OEAP.

Paso 1. Después de que el AP se una al WLC, cambie el modo AP a **FlexConnect** y haga clic en **Aplicar**.

ւլիւլիւ cısco	MONITOR WLANS	Controller Wireless Security M	IANAGEMENT COMMANDS HELP	FEEDBACK
Wireless	All APs > Details for	or AP3800_E1.3EB8		
Access Points All APs	General Crede	ntials Interfaces High Availability	Inventory Advanced I	ntelligent Capture
	General		Versions	
802.11b/g/n/ax	AP Name	AP3800_E1.3E88	Primary Software Version	8.10.130.0
Dual-SG Radios	Location	default location	Backup Software Version	8.10.120.0
Global Configuration	AP MAC Address	70:db:98:e1:3e:b8	Predownload Status	None
Advanced	Base Radio MAC	00:27:e3:36:5a:60	Predownloaded Version	None
Mesh	Admin Status	Enable ¥	Predownload Next Retry Time	NA
AP Group NTP	AP Mode	local V	Predownload Retry Count	NA
ATF	AP Sub Mode	local ElexConnect	Boot Version	1.1.2.4
RF Profiles	Operational Status	monitor	IOS Version	8.10.130.0
FlexConnect Groups	Port Number	Bridge	Mini IOS Version	0.0.0.0
FlexConnect ACLs	Venue Group	Flex+Bridge	IP Config	
ElexConnect VI AN	Venue Type	Unspecified V	CAPWAP Preferred Mode	Ipv4 (Global Config)
Templates	Add New Venue		DHCP Iov4 Address	192.168.100.12
Network Lists	Language Name		Static IP (Iov4/Iov6)	
▶ 802.11a/n/ac/ax	Network Spectrum	3D1781A0FFFC6B2F174A6EF605FB1DF8	Fabric	

Paso 2. Asegúrese de tener al menos un WLC primario configurado en la pestaña Alta Disponibilidad:

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
Wireless	All APs > Details for AP9120_4C.E77C
Access Points All APs Direct APs	General Credentials Interfaces High Availability Inventory FlexConnect Advanced Intelligent Capture
 Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios Dual-SG Radios Cichal Coefficientico 	Name Management IP Address(Ipv4/Ipv6) Primary Controller c3504-01 Secondary Controller I92.168.1.14
 Advanced Mesh 	AP Failover Priority
 AP Group NTP ATF RF Profiles 	
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates	

Paso 3. Vaya a la ficha FlexConnect y marque la casilla de verificación Enable OfficeExtend AP.

	ာါကျက cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
W	ïreless	All APs > Details for AP3800_E1.3EB8
Ŧ	Access Points All APs	General Credentials Interfaces High Availability Inventory FlexConnect Advanced Intelligent Capture
	 Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios 	VLAN Support Make VLAN AP Specific V Go
	Dual-SG Radios Global Configuration	Inheritance Group-Specific
÷	Advanced Mesh	FlexConnect default-flex-group default-flex-group
Þ	AP Group NTP	WILAN AVC Mapping
÷	ATF	VLAN Template Name none
	RF Profiles	VLAN Name Id Mappings
	FlexConnect Groups	
÷	FlexConnect ACLs	PreAuthentication Access Control Lists
	FlexConnect VLAN Templates	External WebAuthentication ACLs
	Network Lists	Costal 2017 Acad
×	802.11a/n/ac/ax	
•	802.11b/g/n/ax	
Þ	Media Stream	OfficeExtend AP
÷	Application Visibility And Control	Enable OfficeExtend AP
	Lync Server	Enable Least Latency Controller Join
	Country	Reset Personal SSID
	Timers	Tunnel Gateway List
	Netflow	
	005	Total

El **cifrado de datos** DTLS se habilita automáticamente cuando habilita el modo OfficeExtend para un AP. Sin embargo, puede habilitar o inhabilitar el cifrado de datos DTLS para un AP específico. Para hacerlo, marque (activar) o desmarque (desactivar) la casilla de verificación **Cifrado de datos** en la ficha Todos los AP > Detalles para [AP seleccionado] > Opciones avanzadas:

ireless	All APs > Deta	ils for AP91	20_4C.E77C				_				
Access Points All APs	General	redentials	Interfaces H	igh Availability	Inventory	FlexConnect	Advanced	Network Diagnost	ics Intelligent Capture		
Direct APs ♥ Radios 802.11a/n/ac/ax	Regulatory Do	mains		802.11bg:-/	802.11a:-B		Power Over	Ethernet Settings			
802.11b/g/n/ax	Country Code			US (United	States) 🗸		PoE Statu	s Fi	ull Power		
Dual-5G Radios	Cisco Discover	ry Protocol					Pre-stand	ard 802.3af switches 🗌)		
Global Configuration	AP Group Nam	ne		FlexOEAP_G	aroup 🗸		Power Injector State				
Advanced	Data Encountin		30			AP Core Dump					
Mesh	Rogue Detection						AP Core Dump				
AP Group NTP				Clabal Conf			AP Retransmit Config Parameters				
ATF				Giobal Com			AP Retransmit Count 5				
RF Profiles	SSH SSH			AP Specific			AP Retran	smit Interval 3	10		
FlexConnect Groups	NSI Ports Stat	te		Global Conf	Global Config 💙			VIAN Tagging			
FlexConnect ACLs	TCP Adjust MS	SS (IPv4: 536 -	1363, IPv6: 1220 - 13	331) III 1250	is Globally Enable	4	VLAN Tagging Enabled NTP Server Status Status Disabled TrustSec				
FlexConnect VLAN Templates	LED State			Enable	 Is clobally chable 						
Network Lists	LED Brightleve	ł		8 (1-8)							
802.11a/n/ac/ax	LED Flash Stat	e		0	(1-3600)seconds						
802.11b/g/n/ax				OIndefinite			TrustSec (Confin			
Media Stream				Oişable			CMY Service	- Control			
Application Visibility	USB Module ID	USB Module ID			USB Module			CHA SERVICES			
And Control	Override						Services S	Sub-Services CMX Ser	ver Ip		
Lync Server	USB Module St	tatus		122							

Nota: El acceso Telnet y SSH se desactivan automáticamente cuando habilita el modo OfficeExtend para un AP. Sin embargo, puede habilitar o inhabilitar el acceso Telnet o SSH para un AP específico. Para hacerlo, marque (activar) o desmarque (desactivar) la casilla de verificación Telnet o SSH en la pestaña All APs > Details for [selected AP] > Advanced . **Nota:** La latencia de link se habilita automáticamente cuando habilita el modo OfficeExtend para un AP. Sin embargo, puede habilitar o inhabilitar la latencia de link para un AP específico. Para hacerlo, marque (activar) o desmarque (desactivar) la casilla de verificación Activar latencia de link en la pestaña Todos los AP > Detalles para [AP seleccionado] > Avanzado.

Paso 3. Seleccione Aplicar. Después de seleccionar Apply (Aplicar), el AP se recarga.

Paso 4. Después de que el AP se reune al WLC, el AP está en el modo OEAP.

Nota: Recomendamos que configure la seguridad de unión de AP (definida comúnmente en Políticas de AP) para que solamente los AP autorizados puedan unirse al WLC. También puede utilizar el aprovisionamiento de puntos de acceso con certificado de importancia local (LSC).

Paso 5. Cree una lista de control de acceso (ACL) de FlexConnect para definir qué tráfico se conmutará de forma centralizada (Denegar) y local (Permitir).

Aquí, tiene el objetivo de cambiar localmente todo el tráfico a la subred 192.168.1.0/24.

	alialia cisco	MONITOR MLANS CON	TROLLER V	VIRELESS SECURIT	Y HUNAGEMENT	COMMANDS HEL	P EEEDBACK		_			
Wireless * Access Points All APs Direct APs * Radios	FlexConnect ACLs > IPv4 ACL > Edit											
	General Access List Name	Fing.0	DEAP_ACL									
	802.11b/g/n/ax Dual-Bend Radios Dual-SG Radios	IP Rules	Action					Protocol	Source Post	Dest Bort	DECP	
	Advanced	1	Permit	0.0.0.0	/ 0.0.0.0	192.168.1.0	/ 255.255.255.0	Any	Any	Any	Any 🖬	
	Mech	2	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any 🗖	
; (AP Group NTP ATF RF Profiles FlexConnect Groups HexConnect ACLS JPv4 AQ, JPv4 AQ, JPv4 AQ, FlexConnect VLAN FlexConnect VLAN Templates	URL Rules Seq Action		Destination Ur	1							

Paso 6. Cree un grupo FlexConnect, vaya al **mapeo ACL** y luego vaya al **mapeo de WLAN-ACL**. En "Local Split ACL Mapping" (Asignación de ACL dividida local), introduzca la ID de WLAN y elija la ACL de FlexConnect. A continuación, haga clic en **Agregar**.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless	FlexConnect Groups > Edit 'FlexConnect_OEAP_Group'
Access Points All APs Direct APs	General Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping WLAN AVC mapping
 Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios Dual-SG Radios Global Configuration 	AAA VLAN-ACL mapping WLAN-ACL mapping Policies Web Auth ACL Mapping Local Split ACL Mapping
 Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups FlexConnect ACLs ElexConnect VIAN 	WLAN Id 0 WebAuth IPV4 ACL none V WebAuth IPv6 ACL none V Add WLAN Add WLAN Profile Name LocalSplit ACL Flex_OEAP_ACL V Add Flex_OEAP_ACL V Id Name ACL ACL ACL Flex_OEAP_ACL V
Templates Network Lists 9 802.11a/n/ac/ax	

Paso 7. Agregue el AP al grupo FlexConnect:

CISCO HONETOR WLANS	ONTROLLER WIRELESS SECURIT	TY MANAGEMENT COMMANDS HELP LEEDBA	ск						
Wireless FlexConnect Group	s > Edit 'FlexConnect_OEAP	_Group'							
* Access Points All APs Direct APs * Balan	uthentication Image Upgrade	ACL Mapping Central DHCP WLAN VLA	N mepping WLAN AVC	mapping					
Proposition of the second	FlexConnect_OEAP_Group								
Advanced Hesh AP Group NTP HTTP-Proxy	vilialia cisco gov Wireless Flax	NTOR WIANS CONTROLLER WIRELESS SECU	RITY МДИЛGEMENT СДИ	MANDS HELP EFEDRACK	1				
R IP Profiles Part FlexConnect Groups * FlexConnect ACLs	Access Points All APS Direct APs v Radios	iroup Name RexConnect_0	EAP_Group						
IP+4 ACL IP+6 ACL ElexConnect VLAN	802.11a/n/ao/ax 802.11b/g/n/ax Dual-Band Radios	xConnect APs	cisco	MONITOR WLANS CONTRO	OLLER WIRELESS SECURITY	маладенент соннал	NOS HELP EEEDBACK		
Templates Server to Address Network Lists Server Type > 002.11a/m/ac/ax Shared Searet > 002.11b/g/m/ax Contem Shared Sea	Dual-3G Rados Global Configuration Add Advanced S Nesh AP Croup NTP et	d AP Select APs from surrent controller AP100 dC 677C thermat benchmark controller Total: 98:e1:Secb5	Wireless * Access Points All APs Direct APs * Radios	FlexConnect Group AP L	ist RexConnect_4	DEAP_Group			
Hedia Stream Port Number Application Visibility And Control Add	ATF RF Profiles FlexConnect Groups E	Add Cancel	802.113/m/36/3x 802.113/g/n/ax Dual-58 Radios Dual-56 Radios Global Configuration	FlexConnect APs					
Lync Server Country	FlexConnect ACLs IPv6 ACL IPv6 ACL FlexConnect VLAN Templates	AP HAC Address AP Name Status	Advanced Hesh AP Group NTP ATF	Select APs from current contro Ethemet HAC	Add Cancel				
	Network Lists		RF Profiles FlexConnect Groups * FlexConnect ACLs IPv4 ACL IPv4 ACL FlexConnect VLAN	Entries 1 - 2 of 2 AP HAC Address 70:db/90:e1:3e:b0 64:f7:d5:4c:e7:7c	AP Name AP300_51.3698 AP9120_4C.677C	Status Associated Associated	AP Hode Reconnect Reconnect	Type Manual Manual	Conflict with PAP No PA

Verificación

1. Verifique el estado y la definición de FlexConnect ACL:

c3504-01) >show flexconnect acl summary
ACL Name Status
Flex_OEAP_ACL Applied
(c3504-01) >show flexconnect acl detailed Flex_OEAP_ACL
Source Destination Source Port Dest Port
Index IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action
1 0.0.0/0.0.0 192.168.1.0/255.255.255.0 Any 0-65535 0-65535 Any Permit
2 0.0.0/0.0.0.0 0.0.0/0.0.0.0 Any 0-65535 0-65535 Any Deny

2. Verifique que la conmutación local de FlexConnect esté inhabilitada:

(c3504-01) >**show wlan 17**

WLAN Identifier..... 17 Profile Name..... FlexOEAP_TEST Network Name (SSID)..... FlexOEAP_TEST Status..... Enabled Interface..... management . . . FlexConnect Local Switching..... Disabled FlexConnect Central Association..... Disabled flexconnect Central Dhcp Flag..... Disabled flexconnect nat-pat Flag..... Disabled flexconnect Dns Override Flag..... Disabled flexconnect PPPoE pass-through..... Disabled flexconnect local-switching IP-source-quar.... Disabled FlexConnect Vlan based Central Switching Disabled FlexConnect Local Authentication..... Disabled FlexConnect Learn IP Address..... Enabled Flexconnect Post-Auth IPv4 ACL..... Unconfigured Flexconnect Post-Auth IPv6 ACL..... Unconfigured . . . Split Tunnel Configuration Split Tunnel..... Disabled Call Snooping..... Disabled Roamed Call Re-Anchor Policy..... Disabled 3. Verifique la configuración del grupo FlexConnect: (c3504-01) >show flexconnect group summary FlexConnect Group Summary: Count: 2 Group Name # Aps ----- -----FlexConnect_OEAP_Group 2 default-flex-group 0

(c3504-01) >show flexconnect group detail FlexConnect_OEAP_Group

______ _____

Number of AP's in Group: 2

AP Ethernet MAC Name Status Mode Type Conflict with PnP

70:db:98:e1:3e:b8 AP3800_E1.3EB8 Joined Flexconnect Manual No c4:f7:d5:4c:e7:7c AP9120_4C.E77C Joined Flexconnect Manual No

Efficient AP Image Upgrade Disabled

Efficient AP Image Join Disabled

Auto ApType Conversion..... Disabled

Master-AP-Mac Master-AP-Name Model Manual

Group Radius Servers Settings: Type Server Address Port _____ Primary Unconfigured Unconfigured Secondary Unconfigured Unconfigured Group Radius/Local Auth Parameters : Active Radius Timeout..... 5 (default) Group Radius AP Settings: AP RADIUS server..... Disabled EAP-FAST Auth..... Disabled LEAP Auth..... Disabled EAP-TLS Auth..... Disabled EAP-TLS CERT Download..... Disabled PEAP Auth..... Disabled Server Key Auto Generated... No Server Key..... <hidden> Authority Info..... Cisco A_ID PAC Timeout..... 0 HTTP-Proxy Ip Address..... HTTP-Proxy Port..... 0 Multicast on Overridden interface config: Disabled DHCP Broadcast Overridden interface config: Disabled Number of User's in Group: 0 FlexConnect Vlan-name to Id Template name: none Group-Specific FlexConnect Local-Split ACLs :

WLAN ID SSID ACL

----- -----

17 FlexOEAP_TEST Flex_OEAP_ACL
Group-Specific Vlan Config:
Vlan Mode..... Enabled
Native Vlan..... 100
Override AP Config..... Disabled
Group-Specific FlexConnect Wlan-Vlan Mapping:

WLAN ID Vlan ID

WLAN ID SSID Central-Dhcp Dns-Override Nat-Pat Puede capturar el tráfico en la interfaz AP para verificar que el tráfico se divide en el AP.

Sugerencia: Para solucionar problemas, puede inhabilitar el cifrado DTLS para ver el tráfico de datos encapsulado dentro del capwap.

Este ejemplo de captura de paquetes muestra el tráfico de datos que coincide con las sentencias ACL "deny" dirigidas al WLC, y el tráfico de datos que coincide con las sentencias ACL "permit" conmutadas localmente en el AP:

File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help
11	10	•	1 25	20	9	0 20 0	4 = =	QQC	11 6	

			A CONTRACT OF A	• • •							
icmp											
No.	Delta		Source	Destination	Length	Info					Ext Tag Number
→	28859	9.819533	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=213/545_	
e	20860	0.019956	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=213/545_	
	20912	0.984274	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=214/547_	
	20913	0.018616	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=214/547_	
	20961	0.986005	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=215/550_	
	20962	0.018343	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=215/558_	
	21007	0.984777	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=216/552_	
	21008	0.018309	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=216/552_	
	21467	9.477613	192.168.1.99	192.168.1.254	74	Echo	(ping)	request	id=0x0001,	seq=217/555	
	21468	0.000638	192.168.1.254	192.168.1.99	74	Echo	(ping)	reply	id=0x0001,	seq=217/555_	
	21511	1.003331	192.168.1.99	192.168.1.254	74	Echo	(ping)	request	id=0x0001,	seq=218/558_	
	21512	0.000192	192.168.1.254	192.168.1.99	74	Echo	(ping)	reply	id=0x0001,	seq=218/558_	
	21572	1.009272	192.168.1.99	192.168.1.254	74	Echo	(ping)	request	id=0x0001,	seq=219/568_	
	21573	0.000000	192.168.1.254	192.168.1.99	74	Echo	(ping)	reply	id=0x0001,	seq=219/560_	
	21621	1.002280	192.168.1.99	192.168.1.254	74	Echo	(ping)	request	id=0x0001,	seq=220/563_	
	21622	0.000374	192.168.1.254	192.168.1.99	74	Echo	(ping)	reply	id=0x0001,	seq=220/563_	

> Frame 20059: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0

> Ethernet II, Src: Cisco_e1:3e:b8 (70:db:98:e1:3e:b8), Dst: Cisco_14:04:b0 (cc:70:ed:14:04:b0)

> Internet Protocol Version 4, Src: 192.168.1.99, Dst: 192.168.1.14

> User Datagram Protocol, Src Port: 5264, Dst Port: 5247

> Control And Provisioning of Wireless Access Points - Data

> IEEE 802.11 Data, Flags:T

> Logical-Link Control

> Internet Protocol Version 4, Src: 192.168.1.139, Dst: 8.8.8.8

> Internet Control Message Protocol

	*Ethernet_yellowCable												
File	e Edit View G	io Capture	Analyze Statistics	Telephony	Wireless Tools	Help							
1	📕 🙇 💿 📃	DXD	۹ 🗢 🗢 🕾 🖗 .	4 🗖 🔳	Q Q Q I								
	imp												
No.	Delt	a s	Source		Destination		Length	Info)				Ext Tag Numb
	20859	9.819533 1	192.168.1.99,192	.168.1.139	192.168.1	.14,8.8.8.8		150 Ech	no (ping)	request	id=0x0001,	seq=213/545_	
	20860	0.019956 1	192.168.1.14,8.8	.8.8	192.168.1	.99,192.168.1.139		142 Ech	no (ping)	reply	id=0x0001,	seq=213/545	
	20912	0.984274 1	192.168.1.99,192	.168.1.139	192.168.1	.14,8.8.8.8		150 Ech	no (ping)	request	id=0x0001,	seq=214/547_	
	20913	0.018616 1	192.168.1.14,8.8	.8.8	192.168.1	.99,192.168.1.139		142 Ech	no (ping)	reply	id=0x0001,	seq=214/547_	
	20961	0.986005 1	192.168.1.99,192	.168.1.139	192.168.1	.14,8.8.8.8		150 Ech	no (ping)	request	id=0x0001,	seq=215/550_	
	20962	0.018343 1	192.168.1.14,8.8	.8.8	192.168.1	.99,192.168.1.139		142 Ech	no (ping)	reply	id=0x0001,	seq=215/550_	
	21007	0.984777 1	192.168.1.99,192	.168.1.139	192.168.1	.14,8.8.8.8		150 Ech	no (ping)	request	id=0x0001,	seq=216/552_	
	21008	0.018309 1	192.168.1.14,8.8	.8.8	192.168.1	.99,192.168.1.139		142 Ech	no (ping)	reply	id=0x0001,	seq=216/552_	
+	21467	9.477613 1	192.168.1.99		192.168.1	.254		74 Ech	no (ping)	request	id=0x0001,	seq=217/555_	
	21468	0.000638 1	192.168.1.254		192.168.1	.99		74 Ech	no (ping)	reply	id=0x0001,	seq=217/555_	
	21511	1.003331 1	192.168.1.99		192.168.1	.254		74 Ech	no (ping)	request	id=0x0001,	seq=218/558_	
	21512	0.000192 1	192.168.1.254		192.168.1	.99		74 Ech	no (ping)	reply	id=0x0001,	seq=218/558_	
	21572	1.009272 1	192.168.1.99		192.168.1	.254		74 Ech	no (ping)	request	id=0x0001,	seq=219/560_	
	21573	0.000000 1	192.168.1.254		192.168.1	.99		74 Ech	no (ping)	reply	id=0x0001,	seq=219/560	
	21621	1.002280 1	192.168.1.99		192.168.1	.254		74 Ech	no (ping)	request	id=0x0001,	seq=220/563	
L.	21622	0.000374 1	192.168.1.254		192.168.1	.99		74 Eck	no (ping)	reply	id=0x0001,	seq=220/563_	

Frame 21467: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: Cisco_e1:3e:b8 (70:db:98:e1:3e:b8), Dst: ThomsonT_73:c5:1d (00:26:44:73:c5:1d)

> Internet Protocol Version 4, Src: 192.168.1.99, Dst: 192.168.1.254

> Internet Control Message Protocol

Nota: En escenarios normales, el AP traduce las direcciones de red para el tráfico conmutado localmente porque la subred del cliente pertenece a la red de la oficina, y los dispositivos locales en la oficina doméstica no saben cómo alcanzar la subred del cliente. El AP utiliza la dirección IP definida en la subred de la oficina local para traducir el tráfico del cliente.

Para verificar que el AP realizó la NAT, puede conectarse al terminal AP y ejecutar el comando "*show ip nat translations*". Ejemplo:

AP3800_E1.3EB8#**show ip nat translations**

(192.168.1.139, 1095, 192.168.1.2, 5000) => (192.168.1.99, 1095, 192.168.1.2, 5000) [*0
gw_h/nat/from_inet_tcp:0] i0 exp85699
...
TCP NAT downstream translations:
(192.168.1.2, 5000, 192.168.1.99, 1223) => (192.168.1.2, 5000, 192.168.1.139, 1223)
[gw_h/nat/to_inet_tcp:0 *0] i0 exp42949165
(192.168.1.2, 5000, 192.168.1.99, 1207) => (192.168.1.2, 5000, 192.168.1.139, 1207)
[gw_h/nat/to_inet_tcp:0 *0] i0 exp85654

Si elimina la tunelización dividida, todo el tráfico se conmuta centralmente en el WLC. Este ejemplo muestra el protocolo de mensajes de control de Internet (ICMP) al destino 192.168.1.2, dentro del túnel capwap:

File E	dit View G	o Capture	Analyze Statistics Telephony	Wireless Tools Help									
4.	0		9.000	Q, Q, Q, II									
icmp													
No.	Delt		Source	Destination	Length	Info					Ext Tag Number	Payload Type	C
-+	108	0.000000	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo ((ping)	request	id=0x0001,	seq=129/330		MSDU	
-	109	0.000046	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo ((ping)	reply	id=0x0001,	seq=129/330		MSDU	
	127	1.000716	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo ((ping)	request	id=0x0001,	seq=130/332		MSDU	
	128	0.000266	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo ((ping)	reply	id=0x0001,	seq=130/332		MSDU	
	142	1.005703	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo ((ping)	request	id=0x0001,	seq=131/335		MSDU	
	143	0.000130	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo ((ping)	reply	id=0x0001,	seq=131/335		MSDU	
	165	1.008894	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo ((ping)	request	id=0x0001,	seq=132/337		MSDU	
	166	0.000133	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo ((ping)	reply	id=0x0001,	seq=132/337		MSDU	

Frame 108: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0 Ethernet II, Src: Cisco_4c:e7:7c (c4:f7:d5:4c:e7:7c), Dst: Cisco_14:04:b0 (cc:70:ed:14:04:b0) Internet Protocol Version 4, Src: 192.168.1.82, Dst: 192.168.1.14 User Datagram Protocol, Src Port: 5251, Dst Port: 5247 Control And Provisioning of Wireless Access Points - Data IEEE 802.11 Data, Flags:T Logical-Link Control Internet Protocol Version 4, Src: 192.168.1.139, Dst: 192.168.1.2 Internet Control Wessage Protocol