Configurar o FlexConnect OEAP com tunelamento dividido

Contents

Introduction Prerequisites Requirements Componentes Utilizados Overview Fatos importantes Configurar Diagrama de Rede Configurações configuração de WLAN Configuração de AP Verificar

Introduction

Este documento descreve como configurar um ponto de acesso (AP) interno como um modo de AP de extensão do escritório (OEAP) FlexConnect e como habilitar o tunelamento dividido para que você possa definir qual tráfego deve ser comutado localmente no escritório doméstico e qual tráfego deve ser comutado centralmente no controlador de LAN sem fio (WLC).

Contribuído por Tiago Antunes, Nicolas Darchis Engenheiros do Cisco TAC.

Prerequisites

Requirements

A configuração neste documento pressupõe que a WLC já está configurada em uma Zona Desmilitarizada (DMZ) com a Conversão de Endereço de Rede (NAT - Network Address Translation) habilitada e que o AP pode ingressar na WLC do escritório de origem.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLCs com versão do software AireOS 8.10(130.0).
- APs Wave1: 1700/2700/3700.
- APs Wave2: séries 1800/2800/3800/4800 e Catalyst 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Um OEAP fornece comunicações seguras de uma WLC Cisco para um AP Cisco em um local remoto, para estender a WLAN corporativa pela Internet para a residência de um funcionário. A experiência do usuário no escritório doméstico é exatamente a mesma que seria no escritório corporativo. A criptografia DTLS (Datagram Transport Layer Security) entre o AP e o controlador garante que todas as comunicações tenham o mais alto nível de segurança. Qualquer AP interno no modo FlexConnect pode atuar como um OEAP.

Fatos importantes

- Os OEAPs da Cisco são projetados para funcionar por trás de um roteador ou outro dispositivo de gateway que usa NAT. O NAT permite que um dispositivo, como um roteador, atue como um agente entre a Internet (pública) e uma rede pessoal (privada), o que permite que um grupo inteiro de computadores seja representado por um único endereço IP. Não há limite para o número de Cisco OEAPs que você pode implantar por trás de um dispositivo NAT.
- Todos os modelos de AP internos suportados com antena integrada podem ser configurados como um OEAP, exceto os AP séries AP-700I, AP-700W e AP802.
- Todos os OEAPs devem estar no mesmo grupo de APs e esse grupo deve conter no máximo 15 LANs sem fio. Um controlador com OEAPs em um grupo de AP publica somente até 15 WLANs para cada OEAP conectado porque reserva uma WLAN para o SSID (Service Set Identifier).

Configurar

Diagrama de Rede



Configurações

configuração de WLAN

Etapa 1. Crie uma WLAN para atribuir ao Grupo AP. Não é necessário habilitar a opção FlexConnect Local Switching para esta WLAN.

ာါကျက cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMAN	DS HELP EEEDBACK
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	HTTP Profiling
	Switching 2 Chebied	PMIP
	FlexConnect Local Auth 12 Enabled	PMIP Mobility Type
	Learn Client IP Address 2 🖾 Enabled	PMIP NAI Type Hexadecimal V
	Vian based Central Enabled 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

Etapa 2. Crie um grupo AP. Na guia **WLANs**, escolha o SSID da WLAN e clique em **Add** para adicionar a WLAN. Vá até a guia **APs** e **adicione** o FlexConnect OEAP.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'
WLANS	General WLANS RF Profile APS 802.11u Location Ports/Module Intelligent Capture
Advanced AP Groups	Add New
	Add New WLAN SSID FlexOEAP_TEST(17) Interface management 1 Group(G) SNMP NAC State Fnabled Add Cancel WLAN ID WLAN SSID ⁽²⁾⁽⁶⁾ Interface Group(G) SNMP NAC State
 cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK



Configuração de AP

Depois que o AP estiver associado ao controlador no modo FlexConnect, você poderá configurá-

lo como um OEAP.

Etapa 1. Depois que o AP ingressar na WLC, altere o modo de AP para **FlexConnect** e clique em **Apply**.

ဂါ၊ဂါ၊ င၊sco	MONITOR WLANS	Controller Wireless Secu	NTY MANAGEME	NT COMMANDS H	elp <u>f</u> eedback
Wireless	All APs > Details f	or AP3800_E1.3EB8			
Access Points All APs	General Crede	ntials Interfaces High Ava	ilability Inve	ntory Advanced	Intelligent Capture
⇒ Radios 802.11a/n/ac/ax	General		Ver	iions	
802.11b/g/n/ax	AP Name	AP3800_E1.3EB8	F	rimary Software Version	8.10.130.0
Dual-5G Radios	Location	default location		ackup Software Version	8.10.120.0
Global Configuration	AP MAC Address	70:db:98:e1:3e:b8	F	redownload Status	None
Advanced	Base Radio MAC	00:27:e3:36:5a:60	F	Predownloaded Version	None
Mesh	Admin Status	Enable ¥	F	Predownload Next Retry Ti	me NA
AP Group NTP	AP Mode	local V	F	Predownload Retry Count	NA
▶ ATF	AP Sub Mode	local FlexConnect	E	loot Version	1.1.2.4
RF Profiles	Operational Status	monitor	I	OS Version	8.10.130.0
FlexConnect Groups	Port Number	Bridge	P	fini IOS Version	0.0.0.0
FlexConnect ACLs	Venue Group	Flex+Bridge v SE-Connect	IP C	onfig	
FlexConnect VLAN	Venue Type Unspecified V			APWAP Preferred Mode	Ipv4 (Global Config)
Templates	Add New Venue			HCP Ipv4 Address	192.168.100.12
Network Lists	Language Name		s	static IP (Ipv4/Ipv6)	
▶ 802.11a/n/ac/ax	Network Spectrum	3D1781A0FFFC6B2F174A6EF605FB1D	8 Fabr	ric	

Etapa 2. Certifique-se de ter pelo menos uma WLC primária configurada na guia Alta disponibilidade:

cisco	Monitor wlans controller wireless security management commands help feedback
Wireless	All APs > Details for AP9120_4C.E77C
* Access Points All APs	General Credentials Interfaces High Availability Inventory FlexConnect Advanced Intelligent Capture
Direct APs * Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios Dual-SG Radios	Name Management IP Address(Ipv4/Ipv6) Primary Controller c3504-01 Secondary Controller 192.168.1.14
Advanced Mesh AP Group NTP	AP Failover Priority Low V
ATF RF Profiles FlexConnect Groups	
 FlexConnect ACLs FlexConnect VLAN Templates Natwork Lists 	

Etapa 3. Vá até a guia FlexConnect e marque a caixa de seleção Enable OfficeExtend AP.

	 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
	Direct APs Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios Dual-SG Radios Global Configuration	VLAN Support Make VLAN AP Specific V Go Inheritance Group-Specific Level Group-Specific
×	Advanced	FlexConnect default-flex-group default-flex-group
	Mesh	WLAN AVC
1		Macong
,	RF Profiles	VLAN rempiate Name none
	FlexConnect Groups	
÷	FlexConnect ACLs	PreAuthentication Access Control Lists
	FlexConnect VLAN Templates	External WebAuthentication AGLs
	Network Lists	Local Self ACLa
×	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

A **Criptografia de Dados** DTLS é ativada automaticamente quando você ativa o modo OfficeExtend para um AP. No entanto, você pode habilitar ou desabilitar a criptografia de dados DTLS para um AP específico. Para fazer isso, marque (habilitar) ou desmarque (desabilitar) a caixa de seleção **Criptografia de dados** na guia Todos os APs > Detalhes de [AP selecionado] > Avançado:

ireless	All APs > Deta	ils for AP91	20_4C.E77C				_				
Access Points	General	redentials	Interfaces H	igh Availability	Inventory	FlexConnect	Advanced	Network Diagnost	ics Intelligent Capture		
Direct APs ♥ Radios 802.11a/n/ac/ax	Regulatory Do		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 Inj	ector State)		
Advanced	Data Encountin	er		30			AP Core Dur	np			
Mesh	Roque Detecti					AP Core Dump Enabled					
AP Group NTP	2 million			Clabal Conf			AP Retransmit Config Parameters				
ATF	- Teinet			Giobal Com			AP Retran	smit Count 5			
RF Profiles	SSH SSH			AP Specific			AP Retran	smit Interval 3	10		
FlexConnect Groups	NSI Ports Stat	te		Global Conf	ig 🗸		VI AN Tanni	10			
FlexConnect ACLs	TCP Adjust MS	SS (IPv4: 536 -	1363, IPv6: 1220 - 13	331) III 1250	is Globally Enable	4			1		
FlexConnect VLAN Templates	LED State			Enable	 Is clobally chable 		NTP Server	ging 🗌	Enabled		
Network Lists	LED Brightleve	ł		8 (1-8)			Status (Disabled			
802.11a/n/ac/ax	LED Flash Stat	e		0	(1-3600)seconds		TrustSec				
802.11b/g/n/ax				OIndefinite			TrustSec (Confin			
Media Stream				Oişable			CMY Service	- Control			
Application Visibility	USB Module ID	USB Module ID					CMA Services				
And Control	Override						Services S	Sub-Services CMX Ser	ver Ip		
Lync Server	USB Module St	tatus		122							

Note: O Telnet e o acesso SSH são desativados automaticamente quando você ativa o modo OfficeExtend para um AP. No entanto, você pode habilitar ou desabilitar o Telnet ou o acesso SSH para um AP específico. Para fazer isso, marque (habilitar) ou desmarque (desabilitar) a caixa de seleção Telnet ou SSH na guia Todos os APs > Detalhes de [AP selecionado] > Avançado.

Note: A latência de link é ativada automaticamente quando você ativa o modo OfficeExtend para um AP. No entanto, você pode ativar ou desativar a latência de link para um AP específico. Para fazer isso, marque (habilitar) ou desmarque (desabilitar) a caixa de seleção Habilitar latência de link em Todos os APs > Detalhes para [AP selecionado] > guia Avançado.

Etapa 3. Selecione Aplicar. Depois de selecionar Aplicar, o AP é recarregado.

Etapa 4. Depois que o AP se junta à WLC, o AP está no modo OEAP.

Note: Recomendamos que você configure a segurança de ingresso do AP (normalmente definida em Políticas de AP) para que somente APs autorizados possam ingressar na WLC. Você também pode usar o provisionamento de AP LSC (Locally Significant Certificate).

Etapa 5. Crie uma lista de controle de acesso (ACL) FlexConnect para definir qual tráfego será comutado centralmente (Negar) e localmente (Permitir).

Aqui, você tem o objetivo de comutar localmente todo o tráfego para a sub-rede 192.168.1.0/24.

	uludu cisco	MONITOR MLANS CO	ONTROLLER	NIRELESS SECUR	ITY MUNAGEMENT	COMMANDS HE	P EEEDBACK					
W	Wireless • Access Points All APs	FlexConnect ACLs >	IPv4 ACL >	Edit								
Ť		General										
	 Radios 802.11a/n/ac/ax 	Access List Neme	fic.)	OBAP_ACL								
	B02.11b/g/n/ex Dual-Band Radios Dual-3G Radios	IP Rules										J
	Global Configuration	Seq	Action	Source IP/Hask		Destination IP/	Hask	Protocol	Source Port	Dest Port	DSCP	J
	Advanced	1	Permit	0.0.0.0	/ 0.0.0.0	192.168.1.0	/ 255.255.255.0	Any	Any	Any	Any 🖸	1
	Mesh	2	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any 🖸	IJ
	AP Group NTP											1
	ATE											
	RF Profiles	URL Rules										
٦	FlexConnect Groups FlexConnect ACLs 1Pv4 AQ.	Seq Action		Destination (ael							
	FlexConnect VLAN Templates											

Etapa 6. Crie um grupo FlexConnect, vá para **Mapeamento de ACL** e vá para **Mapeamento de WLAN-ACL**. Em "Local Split ACL Mapping", digite o ID da WLAN e escolha a ACL FlexConnect. Em seguida, clique em **Adicionar**.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
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	WLAN Id 0 WLAN Id 0 WLAN Id 0 WLAN Id 10 WLA
► AP Group NTP	WebAuth IPv6 ACL none V Add
 ATF RF Profiles FlexConnect Groups 	Add WLAN Id WLAN Profile Name LocalSplit ACL Id Name ACL ACL ACL IT Flex.0EAP_TEST Flex.0EAP_ACL
 FlexConnect ACLs FlexConnect VLAN Templates 	
Network Lists 802.11a/n/ac/ax	

Passo 7. Adicione o AP ao grupo FlexConnect:

cisco	MONITOR WLANS CO	NTROLLER WIRELESS S	ECURITY MANAGEMENT COMMAND	IS HELP LEEDEN	АСК							
Wireless	FlexConnect Groups	>Edit 'FlexConnect_0	OEAP_Group'									
 Access Points All APs Direct APs Radios B02.113/n/ec/ex 802.113/n/ec/ex Dual-Band Radios Dual-56 Radios 	General Local Au Group Name VLAN Template Name	thentication Image Upg PascGareast_OTAP_Ga	grade ACL Mapping Central C	HCP WLAN VLA	AN mopping WLAN AVC	mapping						
Gisbal Configuration Advanced Mesh AD Group NTP ATF	there are constant	viluilu cisco Wireless	MONITOR MIANS CONTROLLER FlexConnect Group AP List	WIRELESS SEC	urity management co	MMANDS HELP EEEDR	NOK					
RF Profiles FlexConnect Groups * FlexConnect ACLs IPv6 ACL IPv6 ACL	Port	 Access Points All APs Direct APs Radius 802.11h/bc/ax 802.11h/p/n/ax 	Group Name	RexConnect_	0649_01000 .1 1.1 1. CISCO	HONITOR MLANS	ONTROLLER WIRELESS	SECURITY MANAGEMEN	IT COMMANDS	HELP ETEDRACK	_	
FlexConnect VLAN Templates Network Lists 9 802.11a/n/ac/ax 9 802.11b/g/n/ax 9 Media Stream Application Visibility	Server tp Address Server Type Shared Secret Confirm Shared Secret Port Number	Dual-Bend Rados Dual-36 Rados Giobal Configuration Advanced Mach A D Group NTP > ATF DE Enofiles	Add AP Selett APs from current centroller AP Nome (AP3000_E1:0888 V) Ethernet (AP300_E1:088 V) Ethernet (AP300_E1:0888 V)	2 75:d: 98:e1:5e:b8 Add Cancel	Wireless * Access Points All APs Einst APs * Radion 802.111/gir/ws Dual-Band Radios	FlexConnect Group Group Name FlexConnect APs	AP List	RexConnect_OEAP_Group				
And Control Lync Server Country	4	FlexConnect Groups FlexConnect ACLs IPv6 ACL IPv6 ACL FlexConnect VLAN Templates	Entries 0 - 0 of 0 AP MAC Address AP Name	Status	Dual-SG Radios Global Configuration Advanced Mesh AP Group NTP ATF	Add AP Select APs from current Ethemet HAC	controller Add Can	al				
		WELWARK LISES			RF Profiles FlexConnect Groups * FlexConnect ACLs IPv6 ACL IPv6 ACL FlexConnect VLAN Templates	Entries 1 - 2: AP MAC Address 701db19010130e1b0 04.171d5140107170	AP Name AP2000_E1.3688 AP9120_4C.677C	Status Associat Associat	ed ed	AP Hode Resident Resident	Type Hanual Hanual	Conflict with PaP No D

Verificar

1. Verifique o status e a definição da ACL do FlexConnect:

c3504-01) >show flexconnect acl summary

2. Verifique se a comutação local FlexConnect está desativada:

(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 Verifique a configuração do 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 Você pode capturar o tráfego na interface do AP para verificar se o tráfego é dividido no AP.

Dica: para fins de solução de problemas, você pode desativar a criptografia DTLS para ver o tráfego de dados encapsulado dentro do capwap.

Este exemplo de captura de pacote mostra o tráfego de dados que corresponde às instruções "deny" da ACL direcionadas para a WLC, e o tráfego de dados que corresponde às instruções "permit" da ACL comutadas localmente no AP:

*Ethernet	t vellow	Cable
 currentee	_yenow	

File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help
16		•	1 25	20	9 00 00	T 20 0	4 = =	000	11 6	

		in and read i	A CONTRACTOR OF A CONTRACTOR O	• • •							
	mp										
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=215/550_	
	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	Edit Viev	Go C	apture	Analyze	Statistics	Telephor	ny Win	eless	Tools	Help										
16	ی کے 🔳			۹ 👄 🖷	1	4 🗐	0	Q, Q	Ξ.											
R komp																				
No.		Delta		Source				Destr	ation				Length	1	Info					Ext Tag Numb
	20859	9.	819533	192.168.	1.99,192	2.168.1.1	39	192.	168.1	.14,8.	8.8.8			150	Echo	(ping)	request	id=0x0001,	seq=213/545_	
	20860	0.	019956	192.168.	1.14,8.8	3.8.8		192.	168.1	.99,19	2.168.1	.139		142	Echo	(ping)	reply	id=0x0001,	seq=213/545_	
	20912	0.	984274	192.168.	1.99,192	2.168.1.1	39	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	3.8.8		192.	168.1	.99,19	2.168.1	.139		142	Echo	(ping)	reply	id=0x0001,	seq=214/547_	
	20961	0.	986005	192.168.	1.99,192	2.168.1.1	39	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	3.8.8		192.	168.1	.99,19	2.168.1	.139		142	Echo	(ping)	reply	id=0x0001,	seq=215/550	
	21007	0.	984777	192.168.	1.99,192	2.168.1.1	39	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	3.8.8		192.	168.1	.99,19	2.168.1	.139		142	Echo	(ping)	reply	id=0x0001,	seq=216/552_	
+	21467	9.4	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	0.0	000192	192.168.	1.254			192.	168.1	.99				74	Echo	(ping)	reply	id=0x0001,	seq=218/558_	
	21572	1.0	009272	192.168.	1.99			192.	168.1	.254				74	Echo	(ping)	request	id=0x0001,	seq=219/560_	
	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_	
L	21622	0.	000374	192.168.	1.254			192.	168.1	.99				74	Echo	(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

Note: Em cenários normais, o AP converte endereços de rede para tráfego comutado localmente porque a sub-rede do cliente pertence à rede do escritório, e os dispositivos locais no escritório doméstico não sabem como acessar a sub-rede do cliente. O AP usa o endereço IP que é definido na sub-rede do home office local para converter o tráfego do cliente.

Para verificar se o AP executou o NAT, você pode se conectar ao terminal do AP e emitir o comando "*show ip nat translations*". Exemplo:

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)

Se você remover o tunelamento dividido, todo o tráfego será comutado centralmente na WLC. Este exemplo mostra o Internet Control Message Protocol (ICMP) para o destino 192.168.1.2, dentro do túnel capwap:

File E	dit View G	o Capture	Analyze Statistics Telephony V	Vireless Iools Help									
1.	0		9 * * * * *										
No.	Delt	а	Source	Destination	Length	Info					Ext Tag Number	Payload Type	d
	108	0.00000	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	
4	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

[gw_h/nat/to_inet_tcp:0 *0] i0 exp85654

т

IEEE 802.11 Data, Flags:

Logical-Link Control

Internet Protocol Version 4, Src: 192.168.1.139, Dst: 192.168.1.2 Internet Control Message Protocol