FlexConnect OEAP met splitter-tunneling configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Overzicht Belangrijke feiten Configureren Netwerkdiagram Configuraties WLAN-configuratie AP-configuratie Verifiëren

Inleiding

In dit document wordt beschreven hoe u een access point (AP) binnen kunt configureren als een FlexConnect Office Extend AP (OEAP)-modus en hoe u splitsingen kunt inschakelen zodat u kunt definiëren wat er lokaal moet worden geschakeld op het thuiskantoor en welk verkeer centraal moet worden geschakeld op de draadloze LAN-controller (WLC).

Bijgedragen door Tiago Antunes, Nicolas Darchis Cisco TAC-engineers.

Voorwaarden

Vereisten

Bij de configuratie van dit document wordt ervan uitgegaan dat de WLC al is geconfigureerd in een gedemilitariseerde zone (DMZ) met netwerkadresomzetting (NAT) en dat AP vanuit het thuiskantoor aan de WLC kan deelnemen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- WLC's met versie AireOS 8.10(130.0) software.
- Wave1 AP's: 1700/2700/3700.
- Wave2 access points: 1800/2800/3800/4800 en Catalyst 9100 Series.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Overzicht

Een OEAP biedt veilige communicatie van een Cisco WLC naar een Cisco AP op een verre plaats, om de bedrijfsWLAN via het internet naar de verblijfplaats van een werknemer uit te breiden. De ervaring van de gebruiker op het thuiskantoor is precies dezelfde als bij het hoofdkantoor. Datagram Transport Layer Security (DTLS)-encryptie tussen de AP en de controller zorgt ervoor dat alle communicatie het hoogste beveiligingsniveau heeft. Elke AP binnen in FlexConnect modus kan als een OEAP fungeren.

Belangrijke feiten

- Cisco OEAP's zijn ontworpen om achter een router of ander gateway-apparaat te werken dat NAT gebruikt. NAT staat een apparaat, zoals een router, toe om als agent tussen het internet (publiek) en een persoonlijk netwerk (privé) te handelen, wat een gehele groep computers toe om door één enkel IP adres vertegenwoordigd te zijn. Er is geen limiet aan het aantal MAP's van Cisco dat u achter een NAT-apparaat kunt implementeren.
- Alle ondersteunde modellen binnen AP met geïntegreerde antenne kunnen als OEAP worden geconfigureerd behalve AP-700I, AP-700W en AP802 reeks AP's.
- Alle OEAP's moeten in dezelfde AP-groep vallen en die groep mag niet meer dan 15 draadloze LAN's bevatten. Een controller met OEAP's in een AP-groep publiceert slechts 15 WLAN's bij elke aangesloten OEAP omdat deze één WLAN-server behoudt voor de persoonlijke serviceset (SSID).

Configureren

Netwerkdiagram



Configuraties

WLAN-configuratie

Stap 1. Maak een WLAN-functie om aan de AP-groep toe te wijzen. U hoeft de FlexConnect Local Switching optie niet in te schakelen voor dit WLAN.

uluulu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMAND	s 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	HTTP Profiling
	Switching 2 Chabled	PMIP
	FlexConnect Local Auth 12 Enabled	PMIP Mobility Type
	Learn Client IP Address 2 🖾 Enabled	PMIP NAI Type Hexadecimal V
	Vlan based Central Enabled	PMIP Profile
	Central DHCP Processing Enabled	PMIP Realm
	Override DNS Enabled	Universal AP Admin Support
	NAT-PAT Enabled	Universal AP Admin
	Central Assoc 🗌 Enabled	11v BSS Transition Support

Stap 2. Maak een AP-groep. Kies in het tabblad **WLAN** de WLAN-sid en klik vervolgens op **Add** om de WLAN-functie toe te voegen. Ga naar het tabblad **AP** en **Voeg** FlexConnect toe.

cisco	MONITOR WLANS CONTROLLER W	IRELESS SECURITY MANAGEMENT	COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Gro	oup'	
VLANs	General WLANs RF Profile	APs 802.11u Location I	Ports/Module Intelligent Capture
Advanced	Add New		Add New
	WLAN SSID FlexOEAP_TEST(1) Interface management Group(G) SNMP NAC State Fnabled Add Cancel WLAN ID WLAN SSID ⁽²⁾⁽⁹⁾ Int	7) V I V I erface/Interface Group(G) SNMP	NAC State
.ı ı.ı ı. cısco	IONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIREL	ess <u>s</u> ecurity m <u>a</u> nagement c <u>o</u> mm	ANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'		
▼ WLANs WLANs	General WLANS RF Profile A	Ps 802.11u Location Ports/M	odule Intelligent Capture
Advanced AP Groups	APs currently in the Group AP Name Ethernet MAC	Remove APs Add APs to the Gr	Oup Add APs Group Name
	AP9120_4C.E77C c4:f7:d5:4c:e7	:7c e:b8	

Nadat de AP met de controller in FlexConnect-modus is gekoppeld, kunt u deze als een OEAP configureren.

Stap 1. Nadat u zich bij de WLC hebt aangesloten, wijzigt u de AP-modus in **FlexConnect** en klikt u op **Toepassen**.

ဂါ၊ဂါ၊ င၊sco	MONITOR WLANS	Controller Wireless Security M	IANAGEMENT COMMANDS HELP	FEEDBACK
Wireless	All APs > Details f	or AP3800_E1.3EB8		
Access Points All APs	General Crede	ntials Interfaces High Availability	Inventory Advanced I	ntelligent Capture
Direct APs ▼ Radios 802.11a/n/ac/ax	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	
ATF	AP Sub Mode	local FlexConnect	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 V	IP Config	
ElexConnect VLAN	Venue Type	Unspecified V	CAPWAP Preferred Mode	Ipv4 (Global Config)
Templates	Add New Venue		DHCP Ipv4 Address	192.168.100.12
Network Lists	Language Name		Static IP (Ipv4/Ipv6)	
802.11a/n/ac/ax	Network Spectrum	3D1781A0FFFC6B2F174A6EF605FB1DF8	Fabric	

Stap 2. Zorg ervoor dat u minimaal een Primaire WLC hebt ingesteld op het tabblad Hoge beschikbaarheid:

cisco	MONITOR WLANS		ess <u>s</u> ecurity ma	NAGEMENT C	OMMANDS HEL	EEEDBACK			
Wireless	All APs > Details fo	or AP9120_4C.E770							
* Access Points All APs	General Creden	itials 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	Primary Controller Secondary	Name c3504-01	Ma 15	Management IP Address(Ipv4/Ipv6) 192.168.1.14					
Global Configuration Advanced	Tertiary Controller		JL						
Mesh AP Group NTP ATF AF Profiles FlexConnect Groups FlexConnect ACLs ElexConnect VI AN	AP Failover Priority	Low							
Templates									

Stap 3. Ga naar het tabblad FlexConnect en controleer het vakje OfficeExtend access point.

	ဂါဂါဂ င၊sco	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	VLAN Support
	Dual-Band Radios Dual-SG Radios Global Configuration	Inheritance Level Group-Specific
÷	Advanced Mesh	FlexConnect default-flex-group default-flex-group
÷	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	Central DVCR Processing
×	802.11a/n/ac/ax	Law 2 40 a
•	802.11b/g/n/ax	
×	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

DTLS **Data Encryption** is automatisch ingeschakeld wanneer u de OfficeExtend-modus voor een AP inschakelen. U kunt echter wel DTLS-gegevensencryptie voor een specifieke AP in- of uitschakelen. Hiervoor controleert u (schakelt u) het aanvinkvakje **Data Encryption** uit op alle AP's > Details voor [geselecteerd AP] > tabblad Advanced:

cisco	MONITOR WLANS CONTROLLER WIRELESS SEC	curity m <u>a</u> nagement c <u>o</u> mmands he <u>l</u> p	<u>F</u> EEDBACK
Wireless	All APs > Details for AP9120_4C.E77C		_
Access Points All APs	General Credentials Interfaces High A	vailability Inventory FlexConnect	Advanced Network Diagnostics Intelligent Capture
Direct APs Radios 802.11a/n/ac/ax 802.11b/g/n/ax	Regulatory Domains Country Code	802.11bg:-A 802.11a:-B US (United States) 🗸	Power Over Ethernet Settings
Dual-Band Radios Dual-SG Radios Global Configuration	Cisco Discovery Protocol AP Group Name	FlexOEAP_Group V	Pre-standard 802.3af switches
Advanced	Statistics Timer	30	AP Core Dump
Mesh	Data Encryption		AR Core Dump
AP Group NTP	Rogue Detection		AP Retransmit Config Parameters
> ATF	² Teinet	Global Config 🗸	
RF Profiles	2 SSH	AP Specific V	AP Retransmit Count 5
FlexConnect Groups	NSI Ports State	Global Config 🗸	VI AN Tagoing
FlexConnect ACLs	TCP Adjust MSS (IPv4: 536 - 1363, IPv6: 1220 - 1331)	TCP MSS is Globally Enabled	
FlexConnect VLAN Templates	LED State		NTP Server Status
Network Lists	LED Brightlevel	8 (1-8)	Status Disabled
802.11a/n/ac/ax	LED Flash State	0 0 (1-3600)seconds	TrustSec
▶ 802.11b/g/n/ax		OIndefinite	TrustSec Config
▶ Media Stream		Disable	CMX Services
Application Visibility And Control	USB Module ID Override	USB Module	Services Sub-Services CMX Server Ip
Lync Server	USB Module Status		
		Contraction of the Contraction o	

Opmerking: Telnet en SSH de toegang worden automatisch uitgeschakeld wanneer u de OfficeExtend modus voor een AP kunt inschakelen. U kunt echter telnet of SSH-toegang voor een specifieke AP in- of uitschakelen. Schakel dit in (schakelt) of uit (schakelt) het selectieteken van telnet of SSH uit op alle AP's > Details voor [geselecteerd AP] > Geavanceerd tabblad.

Opmerking: De latentie van de verbinding wordt automatisch geactiveerd wanneer u de modus OfficeExtend voor een AP toelaat. U kunt echter wel de link latency voor een bepaalde AP inschakelen of uitschakelen. Schakel om dit te doen de optie Link Latency inschakelen in (uitschakelen) of uit het vakje Enable Link Latency in op alle AP's > Details voor [geselecteerde AP] > Geavanceerd tabblad.

Stap 3. Selecteer **Toepassen**. Nadat u Toepassen hebt geselecteerd, herladen de AP opnieuw.

Stap 4. Nadat het AP zich bij de WLC herhaalt, is het AP in de OEAP modus.

Opmerking: We raden u aan om AP aan te sluiten bij veiligheid (algemeen gedefinieerd onder AP Beleid) zodat slechts geautoriseerde APs zich bij de WLC kunnen aansluiten. U kunt ook LSC AP-voorziening (Local Significant certificaatlevering) gebruiken.

Stap 5. Maak een FlexConnect Access Control List (ACL) om te definiëren welk verkeer centraal (Jeans) en lokaal (Permit) zal worden geschakeld.

Hier, hebt u het doel om lokaal al verkeer naar het netto 192.168.1.0/24 te veranderen.

cisco	MONITOR MLANS CO	INTROLLER	WIRELESS SECL	IRITY MANAGEMENT	COMMANDS HE	LP EEEDBACK				
Wireless	FlexConnect ACLs >	IPv4 ACL >	Edit							
All APs	General									
 Radios 802.11a/n/ac/ax 	Access List Neme	fier_	OBAP_ACL							
802.11b/g/n/ex Dual-Band Radios Dual-SC Radios	IP Rules									\neg
Global Configuration	Seq	Action	Source IP/Has	ik .	Destination IP/	/Hask	Protocol	Source Port	Dest Port	DSCP
Advanced	1	Permit	0.0.0.0	/ 0.0.0.0	192.168.1.0	/ 255.255.255.0	Any	Any	Any	Any 🖬
Mesh	2	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Aity 🗖
AP Group NTP										
► ATE										
RF Profiles	URL Rules									
FlexConnect Groups FlexConnect ACLs JPv4 AQL JPv6 ACL	Seq Action		Destination	9 UN						
FlexConnect VLAN										

Stap 6. Maak een FlexConnect-groep, ga naar **ACL-afbeelding** en ga vervolgens naar **WLAN-ACL-**making. Typ onder "Local Split ACL mapping" de WLAN-id en kies FlexConnect ACL. Klik vervolgens op **Toevoegen.**

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 	AAA VLAN-ACL mapping WLAN-ACL mapping Policies Web Auth ACL Mapping Local Split ACL Mapping
Advanced Mesh AP Group NTP ATF	WLAN Id 0 WebAuth IPV4 ACL none V WebAuth IPv6 ACL none Local Split ACL Flex_OEAP_ACL Add MI AN Id
RF Profiles FlexConnect Groups	WLAN WLAN Profile WebAuth IPV4 WebAuth IPV6 17 Flex.0EAP_TEST
 FlexConnect ACLs FlexConnect VLAN Templates Network Lists 	
▶ 802.11a/n/ac/ax	

Stap 7. Voeg AP aan de groep FlexConnect toe:

cisco	MONITOR WLANS C	ONTROLLER WIRELESS S	ECURITY MANAGEMENT COMMAND	S HELP LEEDEN	к						
Wireless	FlexConnect Groups	s > Edit 'FlexConnect_I	OEAP_Group'				1				
Access Points All APa Direct APs Radios	General Local Au	thentication Image Up	grade ACL Mapping Central D	HCP WUAN VU	N mepping WLAN AVC	mapping					
802.11a/n/wo/wx 802.11b/g/n/tox Dual-Band Radios Dual-SG Radios Global Configuration	Group Name VLAN Template Name Enable AP Local Auther	FlaxConnect_ODAP_G	riup								
Advanced Mesh AP Group NTP	HTTP-Proxy	altalta cisco	MONITOR WLANS CONTROLLER	WJRELESS SEC	жіту маладемент со	WWNDS HELP EEEDBAC	×				
ATF RF Profiles FlexConnect Groups FlexConnect ACLs	lp Address(lpv4/lpv4) Part	Access Points All APs Direct APs * Radim	Group Name	RevConnect_	0E4P_Group						
IP+4 ACL IP+6 ACL FlexConnect VLAN Templates	AAA Server in Address	802.11a/n/ac/ax 802.11b/g/n/ex Dual-Band Radios Dual-3G Radios	FlexConnect APs		uluilu cisco Wireless	HONITOR WLANS CO FlexConnect Group A	etroller wijreless secur Plist	ату маладенент сонн	NNDS HELP EEEDBACK		
Network Lists + 802.11a/n/ac/ax + 802.11b/g/n/ax	Server Type Shared Secret Confirm Shared Secre	Advanced Mesh	Add AP Select APs from ourrent controller AP Nome AP3000_61:3688.* Ethernat Name(AP300_6C;677C)	0:d:98:e1:3e:b5	* Access Points All APs Direct APs * Ration	Group Name	RexCon	nect_OEAP_Group			
Media Stream Application Visibility And Control	Port Number	ATF RF Profiles ElevConnect Counts		Add Cancel	802.133/n/ac/ax 802.13b/g/n/ax Dual-Band Radios Dual-55 Radios Clabel Conferentian	FlexConnect APs					
Lync Server Country	4	FlexConnect ACLs IPv6 ACL IPv6 ACL FlexConnect VLAN Templates	AP HAC Address AP Name	Status	Advanced Mesh AP Group NTP	Salact APs from current of Ethemet H4C	Add Cancel	0			
		Network Lists			AIF RF Profiles FlexConnect Groups FlexConnect ACLs Ibst AC	Entries 1 - 2 of AP HAC Address 70:db:90:e1:3e:b0 c4:d7:d5:4c:e7:7c	2 AP Name AP3000_E1.3688 AP9120_40.677C	Status Associated Associated	AP Hode Reconnect	Type Manual Manual	Conflict with PAP
					IPv6 ACL FlexConnect VLAN Templates						

Verifiëren

1. Controleer de status en definitie van 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 0.0.0.0/0.0.0 192.168.1.0/255.255.255.0 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. Controleer dat FlexConnect lokale switching is uitgeschakeld:

(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-guar.... 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 Controleer de configuratie van de FlexConnect-groep:

(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

U kunt het verkeer opnemen op de AP-interface om te controleren of het verkeer gesplitst is op de AP.

Tip: voor probleemoplossing kunt u DTLS-encryptie uitschakelen om het gegevensverkeer in de capwap te zien insluiten.

Dit voorbeeld van de pakketvastlegging toont gegevensverkeer dat de "ontken" van ACL overeenkomt met de verklaringen die op WLC zijn gericht en gegevensverkeer dat de "vergunning" van ACL overeenkomt die lokaal op AP zijn geschakeld:

Cite Edit View

	e con nev	o capture	Analyze sensors responsily the	creas roots rrep									
1	ی کے 🔳		९ 👐 🕫 🗑 🛓 📃 🔍 🍳	ର୍ ବ୍ 🎹									
	l kmp												
No.		Delta	Source	Destination	Length	Info							
\rightarrow	28859	9.819533	3 192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping)	request	id=0x0001,	seq=213/545_				
e	20860	0.019956	5 192.168.1.14,8.8.8.8	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	5 192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping)	reply	id=0x0001,	seq=214/547_				
	20961	0.986005	5 192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping)	request	id=0x0001,	seq=215/550_				
	28962	0.018343	3 192,168,1,14,8,8,8,8	192,168,1,99,192,168,1,139	142	Echo (ping)	reply	id=0x0001.	seq=215/558_				

	20901	0.300003 135.100.1.33,135.100.1.133	192.100.1.14,0.0.0.0	126	ECHO	(brug)	request	10=0x0001,	sed=513/336=	
	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	ame 20059: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0									

Ext Tag Numbe

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

Analyze Statistics Telephony Wiseless Tools Hels

> 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 View	Go	Capture	Analyze	Statistics	Telephon	y Wire	eless Tool	s Help										
A.	ی کے 🔳		XD	9.000	1	A 🗐 🗐	0	Q. Q. 👖											
I imp																			
No.		Delta		Source				Destination	,			Length	1	Info					Ext Tag Numb
	20859	-	9.819533	192.168.	1.99,192	2.168.1.13	9	192.168.	.1.14,8	.8.8.8		3	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	92.168.1.	139	1	142	Echo	(ping)	reply	id=0x0001,	seq=213/545_	
	20912	(0.984274	192.168.	1.99,192	2.168.1.13	9	192.168.	1.14,8	.8.8.8		1	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	92.168.1.	139	1	142	Echo	(ping)	reply	id=0x0001,	seq=214/547_	
	20961	(0.986005	192.168.	1.99,192	2.168.1.13	9	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	92.168.1.	139	1	142	Echo	(ping)	reply	id=0x0001,	seq=215/550_	
	21007	(0.984777	192.168.	1.99,192	2.168.1.13	9	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	92.168.1.	139		142	Echo	(ping)	reply	id=0x0001,	seq=216/552_	
+	21467	9	9.477613	192.168.	1.99			192.168.	1.254				74 1	Echo	(ping)	request	id=0x0001,	seq=217/555_	
	21468	(0.000638	192.168.	1.254			192.168	.1.99				74 1	Echo	(ping)	reply	id=0x0001,	seq=217/555_	
	21511	1	1.003331	192.168.	1.99			192.168.	1.254				74 1	Echo	(ping)	request	id=0x0001,	seq=218/558_	
	21512	(0.000192	192.168.	1.254			192.168.	.1.99				74 1	Echo	(ping)	reply	id=0x0001,	seq=218/558_	
	21572	3	1.009272	192.168.	1.99			192.168	.1.254				74 1	Echo	(ping)	request	id=0x0001,	seq=219/560_	
	21573	(0.000000	192.168.	1.254			192.168	.1.99				74 1	Echo	(ping)	reply	id=0x0001,	seq=219/560_	
	21621	1	1.002280	192.168.	1.99			192.168.	1.254				74 1	Echo	(ping)	request	id=0x0001,	seq=220/563_	
L	21622	4	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

Opmerking: In normale scenario's, vertaalt AP netwerkadressen voor lokaal geschakeld verkeer omdat klink aan het netwerk van het bureau behoort, en de lokale apparaten bij het huisbureau weten niet hoe te om de cliëntesubnet te bereiken. AP gebruikt het IP adres dat in het lokale dienstvoorwerp van het huisbureau wordt gedefinieerd om het clientverkeer te vertalen.

Om te verifiëren dat AP de NAT uitvoerde, kunt u met de AP terminal verbinden en de "*toon ip nat vertalingen*"opdracht geven. Voorbeeld:

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

Als u een gesplitste tunneling verwijdert, is al het verkeer centraal via de WLC geschakeld. Dit voorbeeld toont het Internet Control Message Protocol (ICMP) aan de bestemming 192.168.1.2, binnen de Capwap-tunnel:

File E	dit View (Go Capture	Analyze Statistics Telephony W	/ireless Tools Help									
1.	0		९ 🐵 🖷 🗿 🖉 📃 🖸	1 Q Q II									
i kmpl													
No.	Delt	ta	Source	Destination	Length	Info					Ext Tag Number	Payload Type	(
	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 Message Protocol