# 스플릿 터널링을 사용하여 FlexConnect OEAP 구 성

### 목차

```
소개
<u>사전 요구 사항</u>
<u>요구 사항</u>
<u>사용되는 구성 요소</u>
<u>개요</u>
<u>중요한 사실</u>
<u>구성</u>
<u>네트워크 다이어그램</u>
<u>구성</u>
<u>WLAN 컨피그레이션</u>
<u>다음을 확인합니다.</u>
```

### 소개

이 문서에서는 실내 AP(Access Point)를 FlexConnect Office Extend AP(OEAP) 모드로 구성하는 방법 및 홈 오피스에서 로컬로 스위칭해야 하는 트래픽과 WLC(Wireless LAN Controller)에서 중앙 집중식으로 전환해야 하는 트래픽을 정의할 수 있도록 스플릿 터널링을 활성화하는 방법에 대해 설 명합니다.

기고자: Tiago Antunes, Nicolas Darchis Cisco TAC 엔지니어

## 사전 요구 사항

### 요구 사항

이 문서에는 WLC가 NAT(Network Address Translation)가 활성화된 DMZ(Demilitarized Zone)에 이 미 구성되어 있고 AP가 홈 오피스에서 WLC에 조인할 수 있다고 가정합니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 AireOS 8.10(130.0) 소프트웨어가 포함된 WLC
- Wave1 AP: 1700/2700/3700 .
- Wave2 AP: 1800/2800/3800/4800 및 Catalyst 9100 시리즈입니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

### 개요

OEAP는 인터넷을 통해 기업 WLAN을 직원 거주지로 확장하기 위해 Cisco WLC에서 원격 위치의 Cisco AP로 안전한 통신을 제공합니다. 홈 오피스에서 사용하는 사용자의 경험은 기업 사무실에서 와 정확히 동일합니다. AP와 컨트롤러 간의 DTLS(Datagram Transport Layer Security) 암호화는 모든 통신에서 최고 수준의 보안을 보장합니다. FlexConnect 모드의 모든 실내 AP는 OEAP로 작동 할 수 있습니다.

#### 중요한 사실

- Cisco OEAP는 NAT를 사용하는 라우터 또는 기타 게이트웨이 디바이스에서 작동하도록 설계 되었습니다. NAT를 사용하면 라우터와 같은 장치가 인터넷(공용)과 개인 네트워크(사설) 사이 에서 에이전트 역할을 할 수 있습니다. 이 경우 전체 컴퓨터 그룹을 단일 IP 주소로 나타낼 수 있 습니다. NAT 디바이스 뒤에 구축할 수 있는 Cisco OEAP 수에는 제한이 없습니다.
- 통합 안테나를 사용하는 지원되는 모든 실내 AP 모델은 AP-700I, AP-700W 및 AP802 시리즈 AP를 제외하고 OEAP로 구성할 수 있습니다.
- 모든 OEAP는 동일한 AP 그룹에 있어야 하며, 해당 그룹은 15개 이하의 무선 LAN을 포함해야 합니다. AP 그룹에 OEAP가 있는 컨트롤러는 연결된 각 OEAP에 최대 15개의 WLAN만 게시합 니다. 개인 SSID(Service Set Identifier)에 대해 하나의 WLAN을 예약하기 때문입니다.

### 구성

### 네트워크 다이어그램



#### 구성

#### WLAN 컨피그레이션

1단계. AP 그룹에 할당할 WLAN을 생성합니다. 이 WLAN에 대해 FlexConnect Local Switching 옵 션을 활성화할 필요가 없습니다.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS	HELP EEEDBACK
WLANs	WLANs > Edit 'FlexOEAP_TEST'	
WLANS	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
	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

2단계. AP 그룹을 생성합니다. WLANs(**WLANs**) 탭에서 WLAN SSID를 선택한 다음 Add(**추가**)를 클릭하여 WLAN을 추가합니다. APs(**APs**) 탭**으로** 이동하여 FlexConnect OEAP 추가.

،، ،،، ،، cısco	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
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 <sup>(2)(6)</sup> Interface/Interface Group(G)     SNMP NAC State
alah	
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'
WLANS WLANS	General WLANS RF Profile APs 802.11u Location Ports/Module Intelligent Capture
▼ Advanced	
AP Groups	APs currently in the Group Add APs to the Group Add APs
	AP9120_4C.E77C c4:f7:d5:4c:e7:7c
	AP3800_E1.3E88 70:db:98:e1:3e:b8

#### AP 컨피그레이션

AP가 FlexConnect 모드에서 컨트롤러에 연결되면 이를 OEAP로 구성할 수 있습니다.

1단계. AP가 WLC에 가입하면 AP 모드를 FlexConnect로 변경하고 Apply(적용)를 클릭합니다.

 cısco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY N	IANAGEMENT COMMANDS HELP	EEEDBACK			
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-5G 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				
FlexConnect VLAN	Venue Type	Unspecified ¥	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 Interface Key	3D1781A0FFFC6B2F174A6EF605FB1DF8	Fabric				

### 2단계. High Availability(고가용성) 탭에 최소 1차 WLC가 구성되어 있는지 확인합니다.

/ireless	All APs > Details fo	r AP9120_4C.E770	:							
Access Points All APs	General Creden	tials Interfaces	High Availability	Inventory	FlexConnect	Advanced	Intelligent Capture			
Direct APs * Radios 802.11a/n/ac/ax		Name	Ма	Management IP Address(Ipv4/Ipv6)						
802.11b/g/n/ax Dual-Band Radios	Primary Controller	c3504-01	19	2.168.1.14						
Dual-SG Radios Global Configuration	Tertiary Controller									
Advanced										
Mesh	AP Failover Priority	Low V								
AP Group NTP										
ATF										
RF Profiles										
FlexConnect Groups										
FlexConnect ACLs										
FlexConnect VLAN Templates										

3단계. FlexConnect 탭으로 이동하여 OfficeExtend **AP 사용** 확인란을 선택합니다.

	 cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
W	ireless	All APs > Details for AP3800_E1.3EB8
*	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 Dual-SG Radios Global Configuration	VLAN Support Description Make VLAN AP Specific Go Inheritance Level Group-Specific
+	Advanced Mesh	FlexConnect Group Name 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	Costel 2017 Acad
•	802.11a/n/ac/ax	Law 240 s
•	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

AP에 대해 OfficeExtend 모드를 활성화하면 DTLS 데이터 암호화가 자동으로 활성화됩니다. 그러 나 특정 AP에 대해 DTLS 데이터 암호화를 활성화하거나 비활성화할 수 있습니다. 이렇게 하려면 [선택한 AP]에 대한 [세부 정보] > [고급] 탭의 [모든 AP] > [데이터 암호화] 확인란을 선택(활성화) 또 는 선택 취소(비활성화)(비활성화)합니다.

	cisco		<u>w</u> lans <u>c</u> ontro	OLLER WIRELESS	<u>s</u> ecurity M <u>a</u>	NAGEMENT COM	MANDS HELP	<b><u>F</u>EEDBACK</b>					
W	ireless	All APs > Details for AP9120_4C.E77C											
*	Access Points All APs	General	Credentials	Interfaces	High Availability	Inventory F	lexConnect	Advanced	Network Diagno	stics	Intelligent Capture		
	<ul> <li>Direct APs</li> <li>♥ Radios</li> <li>802.11a/n/ac/ax</li> <li>802.11b/g/n/ax</li> <li>Dual-Band Radios</li> </ul>	Regulator Country (	ry Domains Code		802.11bg:-/	802.11bg:-A 802.11a:-B US (United States) ♥			Power Over Ethernet Settings PoE Status Full Power				
	Dual-SG Radios Global Configuration	AP Group Name			FlexOEAP_G	FlexOEAP_Group V			ard 802.3af switches ector State				
*	Advanced	Statistics	Timer		30			AP Core Dun					
	Mesh AP Group NTP	Rogue De	etection					AP Core D	ump	Enabled			
1	ATE	2 Telnet	:		Global Conf	fig 🗸 🗌		AP Retransmit Config Parameters					
	RF Profiles	2 SSH			AP Specific	<b>v</b>		AP Retran	smit Count	5			
	FlexConnect Groups	NSI Ports	s State		Global Conf	fig 💙 🖾		VLAN Tagging					
•	FlexConnect ACLs	TCP Adju	st MSS (IPv4: 536 ·	- 1363, IPv6: 1220 -	1331) I 1250 TCP MSS	is Globally Enabled		VLAN Tag	d				
	FlexConnect VLAN Templates	LED State			Enable	<b>~</b>		NTP Server					
	Network Lists	LED Brigh	tlevel		8 (1-8)			Status Disabled					
Þ	802.11a/n/ac/ax	LED Flash	State		0 0	(1-3600)seconds		TrustSec					
•	802.11b/g/n/ax							TrustSec 0	Config				
Þ	Media Stream	USB Modu	ule ID		USB Module			CMX Service	s				
•	Application Visibility And Control	Override							Services Sub-Services CMX Server Ip				
	Lync Server	USB Modu	ule Status		12								

**참고:** AP에 대해 OfficeExtend 모드를 활성화하면 텔넷 및 SSH 액세스가 자동으로 비활성화 됩니다. 그러나 특정 AP에 대해 텔넷 또는 SSH 액세스를 활성화 또는 비활성화할 수 있습니 다. 이렇게 하려면 [선택한 AP] > [고급] 탭의 [모든 AP] > [세부 정보]에서 텔넷 또는 SSH 확인 란을 선택(활성화)하거나 선택 취소(비활성화)합니다. **참고:** AP에 대해 OfficeExtend 모드를 활성화하면 링크 레이턴시가 자동으로 활성화됩니다. 그러나 특정 AP에 대해 링크 레이턴시를 활성화하거나 비활성화할 수 있습니다. 이렇게 하려 면 All APs(모든 AP) > Details for [selected AP](선택한 AP] > Advanced(고급) 탭에서 Enable Link Latency(링크 레이턴시 활성화) 확인란을 선택(활성화) 또는 선택 취소(비활성화)합니다.

3단계. 적용을 선택합니다. Apply(적용)를 선택하면 AP가 다시 로드됩니다.

4단계. AP가 WLC에 다시 연결되면 AP는 OEAP 모드에 있습니다.

**참고:** 인증된 AP만 WLC에 참여할 수 있도록 AP 가입 보안(일반적으로 AP Policies에 정의됨)을 구성하는 것이 좋습니다. LSC(Locally Significant Certificate) AP 프로비저닝을 사용할 수 도 있습니다.

5단계. FlexConnect ACL(Access Control List)을 생성하여 중앙에서(거부) 및 로컬로(허용)로 전환 할 트래픽을 정의합니다.

여기에서는 모든 트래픽을 서브넷 192.168.1.0/24으로 로컬로 스위칭하는 것을 목표로 합니다.

	uludu cisco	MONITOR MLANS CON	TROLLER	WIRELESS SECURI	Y HAVAGEMENT	COMMANDS HEL	P EEEDBACK								
Wireless	fireless	FlexConnect ACLs > If	FlexConnect ACLs > IPv4 ACL > Edit												
Ť	All APs	General													
	Redice     Redice     Redice     802.11a/n/ac/ax     802.11b/g/n/ex     Dual-Band Radios     Dual-Gand Radios	Access List Name	fier_	OBAP_ACL								_			
		IP Rules										٦			
	<b>Global Configuration</b>	Seq	Action	Source IP/Hask		Destination IP/I	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	Any				
	AP Group NTP											-			
	ATF														
	RF Profiles	URL Rules													
٦	FlexConnect Groups FlexConnect ACLS 1Pv4 AQL 1Pv5 AQL	Seq Action Destination Uni													
	FlexConnect VLAN Templates														

6단계. FlexConnect 그룹을 생성하고 ACL 매핑으로 이동한 다음 WLAN-ACL 매핑으로 이동합니다 . "Local Split ACL Mapping(로컬 스플릿 ACL 매핑)"에서 WLAN ID를 입력하고 FlexConnect ACL을 선택합니다. 그런 다음 Add를 클릭합니다.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
Wireless	FlexConnect Groups > Edit 'FlexConnect_OEAP_Group'
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Direct APs</li> </ul> </li> </ul>	General Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping WLAN AVC mapping
<ul> <li>Radios</li> <li>802.11a/n/ac/ax</li> <li>802.11b/g/n/ax</li> <li>Dual-Band Radios</li> <li>Dual-SG Radios</li> <li>Global Configuration</li> </ul>	AAA VLAN-ACL mapping WLAN-ACL mapping Policies Web Auth ACL Mapping Local Split ACL Mapping
<ul> <li>Advanced Mesh</li> <li>AP Group NTP</li> <li>ATF RF Profiles FlexConnect Groups</li> <li>FlexConnect ACLs FlexConnect VLAN Templates Network Liets</li> </ul>	WLAN Id       0         WebAuth IPV4 ACL none       wilan Id         WebAuth IPv6 ACL       none         Add       Add         WLAN WLAN Profile       WebAuth IPV4         WebAuth IPV4       WebAuth IPV6         AcL       WLAN Id         Id       WLAN Id         VIAN WLAN Profile       WebAuth IPV4         ACL       FlexOBAP_TEST         Id       Flex_OEAP_ACL<
<ul> <li>802.11a/n/ac/ax</li> </ul>	

7단계. FlexConnect 그룹에 AP를 추가합니다.

	MONITOR MLANS CO	ONTROLLER WIRELESS 5	ECURITY MANAGEMENT COMMANDS	HELP FEEDO	кск						
Wireless	FlexConnect Groups	>Edit 'FlexConnect_	OEAP_Group'								
Access Points     All APs     Direct APs     Profes	General Local Au	thentication Image Up	grade ACL Mapping Central DH	CP WLAN VU	AN mepping WLAN AVC	mepping					
B02.11a/n/ed/ex B02.11b/g/n/ox Dual-Band Radios Dual-SG Radios Global Configuration	Group Name VLAN Template Name Erable AP Local Author	MaxConnect_ODAP_G	resp								
Advanced     Mesh     AP Group NTP	HTTP-Proxy	սիսիս cisco	MONITOR WLANS CONTROLLER	WIRELESS SEC	urity management co	WWNDS HELP EEEDBW	×				
ATF     RF Profiles     FlexConnect Groups     FlexConnect A(1)	lp Address(lpv4/lpv4) Part	Access Points     All APs     Direct APs	Group Name	RexConnect_	OEAP_Group						
IP+4 ACL IP+6 ACL FlexConnect VLAN Templates	AAA Server Ip Address	<ul> <li>Ration</li> <li>802.11b/tr/bo/ax</li> <li>802.11b/g/v/ax</li> <li>Dual-Gend Radios</li> <li>Dual-SG Radios</li> <li>Global Configuration</li> </ul>	FlexConnect APs		uluulu cisco Wireless	MONITOR WLANS CO	rtroller wijkeless secu P List	RITY MANAGEMENT COMM	ANDS HELP ETEDBACK		
Network Lists > 802.11a/n/ac/ax > 802.11b/g/n/ax	Server Type Shared Secret Confirm Shared Secre	Advanced     Mesh     AP Group NTP	Select APa from current controller	) :db:98:e1:3e:b8	Access Points     All APs     Direct APs     v Ration	Group Name	PexCo	nnect_OEAP_Group			
Media Stream     Application Visibility     And Control	Port Number	ATF     RF Profiles     FlexConnect Groups	Entries 0 - 0 of 0		802.133/n/36/38 802.13b/g/n/ex Dual-Band Radios Dual-SG Radios Global Configuration	FlexConnect APs					
Country	4	<ul> <li>FlexConnect ACLs IPv4 AQ, IPv6 ACL     </li> <li>FlexConnect VLAN     </li> </ul>	AP HAC Address AP Neme	Status	Advanced     Hesh     AP Group NTP	Salact APs from current o Ethernet HAC	Add Cancel				
		Network Lists			ATF     RF Profiles     FlexConnect Groups     FlexConnect ACLs	Entries 1 - 2 of AP HAC Address 701db:901e313e1b0 c4:d71d51d1e272c	2 AP Name AP300_E1.3688 AP1120_4C.672C	Status Associated	AP Hode Reconnect	Type Manual	Conflict with PAP
					IPV6 ACL FlexConnect VLAN Templates						

### 다음을 확인합니다.

1. FlexConnect ACL 상태 및 정의를 확인합니다.

c3504-01) >show flexconnect acl summary

ACL Name Status

----- -----

Flex\_OEAP\_ACL Applied

(c3504-01) >show flexconnect acl detailed Flex\_OEAP\_ACL

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

WLAN Identifi	.er	17
Profile Name.		FlexOEAP_TEST
Network Name	(SSID)	FlexOEAP_TEST
Status		Enabled
•••		
Interface		management
FlexConnect I	ocal Switching	Disabled
FlexConnect C	Central Association	Disabled
flexconnect C	Central Dhcp Flag	Disabled
flexconnect C flexconnect r	Central Dhcp Flag Nat-pat Flag	Disabled Disabled
flexconnect C flexconnect r flexconnect I	Central Dhcp Flag Nat-pat Flag Mns Override Flag	Disabled Disabled 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. FlexConnect 그룹 구성을 확인합니다. (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 TO Vlan TD

Fthemet vellowCable

\_\_\_\_\_

WLAN ID SSID Central-Dhcp Dns-Override Nat-Pat AP 인터페이스에서 트래픽을 캡처하여 트래픽이 AP에서 분할되었는지 확인할 수 있습니다.

팁: 문제 해결을 위해 DTLS 암호화를 비활성화하면 CAPWAP 내에서 캡슐화된 데이터 트래 픽을 볼 수 있습니다.

이 패킷 캡처 예에서는 WLC로 전달되는 ACL "deny" 문과 일치하는 데이터 트래픽과 AP에서 로컬 로 전환된 ACL "permit" 문과 일치하는 데이터 트래픽을 보여줍니다.

_	contract ferret					
File	Edit View Go	Capture	Analyze Statistics Telephony	Wireless Tools Help		
st.	📕 🙇 🛞 🛄 🗖	XC	९ 👐 🗢 🕾 Ŧ 🛓 🚍 🔳	Q, Q, Q, 🔢		
	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=219/560_
	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_
	21622	0.000374	192.168.1.254	192.168.1.99	74 Echo (ping) reply	id=0x0001, seq=220/563_

> Frame 20859: 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

4	🧧 *Ethernet_yellowCable											
Fi	le Edit View Go	Capture	Analyze Statistics Telephony	Wireless Tools H	elp							
1	( 🔳 🧟 💿 📃 🗄	XD	९ 👄 🗢 🕾 🖗 🚊 🚍	ର୍ ର୍ ଷ୍ 🎹								
	iomp											
No	. Delta		Source	Destination		Length	Info					Ext Tag Numb
1	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_	
	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	192.168.1.25	54	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	192.168.1.25	i4	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	192.168.1.25	54	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	192.168.1.25	i4	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

**참고:** 일반적인 시나리오에서 AP는 클라이언트 서브넷이 사무실 네트워크에 속하고, 홈 오피 스의 로컬 디바이스는 클라이언트 서브넷에 도달하는 방법을 모르기 때문에 로컬로 스위칭된 트래픽의 네트워크 주소를 변환합니다. AP는 로컬 홈 오피스 서브넷에 정의된 IP 주소를 사용 하여 클라이언트 트래픽을 변환합니다.

AP가 NAT를 수행했는지 확인하기 위해 AP 터미널에 연결하고 "*show ip nat translations*" 명령을 실 행할 수 있습니다. 예:

#### AP3800\_E1.3EB8#show ip nat translations

TCP NAT upstream translations: (192.168.1.139, 1223, 192.168.1.2, 5000) => (192.168.1.99, 1223, 192.168.1.2, 5000) [\*0 gw\_h/nat/from\_inet\_tcp:0] i0 exp42949165 (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

스플릿 터널링을 제거하면 WLC에서 모든 트래픽이 중앙에서 전환됩니다. 다음 예에서는 capwap 터널 내부의 192.168.1.2 대상에 대한 ICMP(Internet Control Message Protocol)를 보여 줍니다.

File E	dit View G	o Capture	Analyze Statistics Telephony V Q @ @ @ 2 1 2 2 2 0 0	Vireless Tools Help Q Q III						
kompl										
No.	Delta	P	Source	Destination	Length	Info				
	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
-	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
	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
	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
	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
	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
	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
	166	0.000133	192,168,1,14,192,168,1,2	192,168,1,82,192,168,1,139	142	Echo	(ning)	reply	id=0x0001.	seg=132/337

Ext Tag Number

Payload Type

MSDU MSDU MSDU MSDU MSDU

MSDU MSDU

MSDU

Ch

> 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