# Konfigurationsbeispiel für Catalyst 9800 und FlexConnect OEAP Split Tunneling

## Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Überblick Hintergrundinformationen Konfigurieren Netzwerkdiagramm Konfigurationen Definieren einer Zugriffskontrollliste für Split Tunneling Verknüpfen einer ACL-Richtlinie mit der definierten ACL Konfigurieren einer Wireless-Profilrichtlinie und eines Split MAC ACL-Namens Zuordnen eines WLAN zu einem Richtlinienprofil Konfigurieren eines AP-Join-Profils und der Verknüpfung mit dem Site-Tag Anfügen eines Richtlinien-Tags und eines Site-Tags an einen Access Point Überprüfung **Zugehörige Dokumentation** 

## Einleitung

Dieses Dokument zeigt, wie der WLC 9800 mit Access Points für Innenbereiche im FlexConnect Office Extend (OEAP)-Modus konfiguriert und Split-Tunneling aktiviert wird, um festzulegen, welcher Datenverkehr lokal im Heimbüro geswitcht werden kann und welcher Datenverkehr zentral am WLC weitergeleitet und geschaltet werden sollte.

## Voraussetzungen

## Anforderungen

Bei der Konfiguration in diesem Dokument wird davon ausgegangen, dass der WLC bereits in einer DMZ mit aktivierter NAT konfiguriert ist und dass der Access Point vom Heimbüro aus dem WLC beitreten kann.

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

• Wireless LAN Controller 9800 mit IOS-XE 17.3.1 Software

- Wave1-APs: 1700/2700/3700.
- Wave2-APs: 1800/2800/3800/4800 und der Catalyst Serie 9100.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung.

Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

# Überblick

Ein Cisco OfficeExtend Access Point (Cisco OEAP) bietet eine sichere Kommunikation von einem Cisco WLC zu einem Cisco AP an einem Remote-Standort und erweitert nahtlos das Unternehmens-WLAN über das Internet auf den Wohnsitz eines Mitarbeiters. Das Anwendererlebnis im Heimbüro ist genauso wie im Büro. Die DTLS-Verschlüsselung (Datagram Transport Layer Security) zwischen Access Point und Controller stellt sicher, dass alle Kommunikationen ein Höchstmaß an Sicherheit bieten. Jeder Access Point in Innenräumen in FlexConnect kann als Office Extend AP fungieren.

### Hintergrundinformationen

FlexConnect bezieht sich auf die Fähigkeit eines Access Points (AP), Wireless-Clients zu verwalten, während diese an entfernten Standorten betrieben werden, z. B. über ein WAN. Sie können auch entscheiden, ob der Datenverkehr von den Wireless-Clients direkt auf der AP-Ebene (Lokales Switching) in das Netzwerk geleitet wird oder ob der Datenverkehr zentralisiert an den 9800-Controller (Central Switching) geleitet und auf WLAN-Basis über das WAN zurückgesendet wird.

Weitere Informationen zu FlexConnect finden Sie in diesem Dokument <u>Verstehen von</u> <u>FlexConnect auf Catalyst 9800 Wireless Controller</u>.

Der Office Extend-Modus ist eine Option, die in einem FlexConnect-Access Point verfügbar ist, um zusätzliche Funktionen bereitzustellen, z. B. eine persönliche lokale SSID für den Heimzugriff, und kann auch Split-Tunneling-Funktion bereitstellen, um detaillierter festzulegen, welcher Datenverkehr lokal im Heimbüro und welcher Datenverkehr zentral im WLC über ein einzelnes WLAN geschaltet werden soll.

## Konfigurieren

Netzwerkdiagramm



### Konfigurationen

### Definieren einer Zugriffskontrollliste für Split Tunneling

Schritt 1: Wählen Sie Configuration > Security > ACL aus. Klicken Sie auf Hinzufügen.

Schritt 2: Geben Sie im Dialogfeld Add ACL Setup (ACL-Einrichtung hinzufügen) den ACL-Namen ein, wählen Sie in der Dropdown-Liste ACL Type (ACL-Typ) den ACL-Typ aus, und geben Sie unter Rules settings (Regeleinstellungen) die Sequenznummer ein. Wählen Sie dann Aktion entweder als Zulassen oder Ablehnen aus.

Schritt 3: Wählen Sie in der Dropdown-Liste Source Type (Quellentyp) den gewünschten Quelltyp aus.

Wenn Sie den Quelltyp als Host auswählen, müssen Sie den Hostnamen/die IP-Adresse eingeben.

Wenn Sie den Quelltyp als Netzwerk auswählen, müssen Sie die Quell-IP-Adresse und die Platzhaltermaske angeben.

In diesem Beispiel wird der gesamte Datenverkehr von einem Host zum Subnetz 192.168.1.0/24 zentral umgeleitet (verweigern), und der restliche Datenverkehr wird lokal geschaltet (zulassen).

Cisco Catalyst 9	800-CL Wireless Co	ntroller	Welcome admin		Search APs and Clients Q	
Q Search Menu Items	nfiguration * > Security *	> ACL				
Dashboard	+ Add X. Delete	Associate Interfaces				
	d ACL Setup					× .
A Monitoring	CL Name*	HomeOffice_ACL	ACL Type	IPv4 Extended 🔹		
Configuration > R	tules					
S Administration	equence*	1	Action	deny 🔹		
C Licensing	ource Type	any 🔻				
X Troubleshooting D	estination Type	Network 🔻				
D	estination IP*	192.168.1.0	Destination Wildcard*	0.0.0.255		
P	rotocol	p v				
L	og	Ø	DSCP	None		
	+ Add × Delete	l .				
	Sequence ~ Action	<ul> <li>Source IP</li> <li>Source IP</li> <li>Wildcard</li> </ul>	Destination ~ Destination ~ Wildcard	Protocol ~ Port	Port DSCP v Log	, ~
	⊲ ⊲ 0 ⊳ ⊳	10 🔻 items per page			No items to disp	xay
	D Cancel				Apply to Dev	ice

Schritt 4: Aktivieren Sie das Kontrollkästchen Protokoll, wenn Sie die Protokolle speichern möchten, und klicken Sie auf Hinzufügen.

Schritt 5: Fügen Sie die übrigen Regeln hinzu, und klicken Sie auf Auf Gerät anwenden.

🛄 Apps 📙 My 📄 PersonalAdmin 🦲 W	VorkAndVac 🧧 WebMons 🔒	Shifts Community PS	HTTS Wir 11AX el	WLC 🚺 DNA 📃 LAB 🛄	Home Lab 🧧 WNBU 🚺 Ad	c »
Cisco Cisco Catalyst	9800-CL Wireless Co	ontroller	Welcome admin 🛛 縃 🤻		Soarch APs and Cliente C	2 🛛
Q. Sisarch Meno Items	nfiguration * > Security * + Add × Delete	ACL     Associate Interfaces				
Ad	ld ACL Setup					×
C Monitoring	ACL Name*	HomeOffice_ACL	ACL Type	IPv4 Extended 🔹 👻		
Sconfiguration	Rules					
€ Administration →	Sequence*	ī ī	Action	permit 🗸		
C Licensing	Source Type	any				
💥 Troubleshooting	Destination Type	any 👻				
F	Protocol	ahp 🔹				
	.og	0	DSCP	None 🖌		
	+ Add X Delete	1				
	Sequence ~ Action	v IP Source v Wildcard	Destination ~ Destination ~ Wildcard	Protocol ~ Port	Destination ~ Port DSCP ~	Log ~
	O 1 deny	any	192.168.1.0 0.0.0.255	ip None	None None	Enabled
	O 2 permit	any	any	ip None	None None	Disabled
	4 4 1 ⊨ ⊨  [	10 🔻 items per page			1 - 2 of	2 items
	Cancel				Apply to	Device

Verknüpfen einer ACL-Richtlinie mit der definierten ACL

Schritt 1: Erstellen Sie ein neues Flex-Profil. Gehen Sie zu Konfiguration > Tags & Profile > Flex.

Klicken Sie auf Hinzufügen.

Schritt 2: Geben Sie einen Namen ein, und aktivieren Sie Office Extend AP. Stellen Sie außerdem sicher, dass die native VLAN-ID die im AP-Switch-Port ist.

Cisco Catalyst 98	00-CL Wireless Controller			Welcome admin	C 0 0 0 0 0	Search Alf4 and Classis Q
Config Dashboard	Add Control Co	ion Policy ACL VLAN	Umbrella		×	
Configuration Administration Configuration	<ul> <li>Name*</li> <li>Description</li> <li>Native VLAN ID</li> <li>HTTP Praxy Port</li> <li>HTTP-Praxy IP Address</li> <li>CTS Policy</li> <li>Inline Tagging</li> <li>SGACL, Enforcement</li> <li>CTS Profile Name</li> </ul>	HomeOffice_PlexProfile Enter Description 1 0 0.0.0.0 default-sxp-profile_N •	Fallback Radio Shut Flex Resilient ARP Caching Efficient Image Upgrade Office Extend AP Join Minimum Latency mDNS Flex Profile	O O O Search or Select		
	Cancel			8	Apply to Device	

**Anmerkung:** Wenn Sie den Office-Extend-Modus aktivieren, ist die Link-Encryption ebenfalls standardmäßig aktiviert und kann nicht geändert werden, selbst wenn Sie die Link-Verschlüsselung im AP-Join-Profil deaktivieren.

Schritt 3: Wechseln Sie zur Registerkarte "Policy ACL", und klicken Sie auf Hinzufügen. Fügen Sie hier die ACL zum Profil hinzu, und wenden Sie sie auf das Gerät an.

¢	cisco	Cisco Catalyst 9800-CL W	/ireless Controller	Weid	come admin	*	6	• 3	02	Search APs and Clients
Q	Search Menu I	Configuration * >	Tags & Profiles * > Flex							
		Add Flex Profile								×
G		General Local Authentic	cation Policy ACL VL	AN Umbrella						
2		T Adu X Delete	F	Pre Auth URL						
<u>ک</u>		ACL Name HomeOffice_ACL	<ul> <li>Central Web Auth ~ F</li> <li>Disabled</li> </ul>	ilter						
C			items per page	1 - 1 of 1 items						
X		Cancel								Apply to Device

#### Konfigurieren einer Wireless-Profilrichtlinie und eines Split MAC ACL-Namens

Schritt 1: Erstellen Sie ein WLAN-Profil. In diesem Beispiel wurde eine SSID mit dem Namen HomeOffice mit WPA2-PSK-Sicherheit verwendet.

Schritt 2: Erstellen eines Richtlinienprofils Gehen Sie zu Konfiguration > Tags > Richtlinie, und

klicken Sie auf Hinzufügen. Stellen Sie unter Allgemein sicher, dass dieses Profil zentral geswitchte Richtlinien hat, wie in diesem Beispiel gezeigt:

Search Menu Items	General Access Policies	QOS and AVC Mobility	Advanced	
	A Config	uring in enabled state will result in loss	of connectivity for clients associated wi	th this profile.
	Name*	HomeOfficePolicy	WLAN Switching Policy	
Administration	Description	Enter Description	Central Switching	
	Status		Central Authentication	
	Passive Client Encrypted Traffic Analytics	DISABLED DISABLED	Central DHCP Central Association	ENABLED DISABLED
	CTS Policy		Flex NAT/PAT	DISABLED
	Inline Tagging	O		
	SGACL Enforcement	0		
	Default SGT	2-65519		

Schritt 3: Gehen Sie im Richtlinienprofil zu Access Policies (Zugriffsrichtlinien), und definieren Sie das VLAN für den Datenverkehr, der zentral geswitcht werden soll. Die Clients erhalten die IP-Adresse im Subnetz, das diesem VLAN zugewiesen ist.

Cisco Catal	yst 9800-CL Wireless Cont	roller Wei	come admin   縃 📽 🖺 🏟 🙆	Search APs and Clients Q
Q Search Menu Items	+ Add × Delete	General Access Policies	QOS and AVC Mobility Advanced	
Monitoring	Status V Policy Profile Nam	RADIUS Profiling	0	WLAN ACL
Configuration	HomeOfficePolic	DHCP TLV Caching	0	IPv6 ACL Search or Select
Administration		WLAN Local Profiling		URL Filters
C Licensing	□ ♥ ······	Global State of Device Classification	Disabled (i)	Pre Auth Search or Select
X Troubleshooting		Local Subscriber Policy Name	Search or Select	Post Auth Search or Select 👻
		VLAN/VLAN Group	default	
		Multicast VLAN	Enter Multicast VLAN	
		Cancel		Tupdate & Apply to Device

Schritt 4: Um lokales Split-Tunneling auf einem WAP zu konfigurieren, müssen Sie sicherstellen,

dass DCHP Required im WLAN aktiviert ist. Dadurch wird sichergestellt, dass der Client, der dem geteilten WLAN zugeordnet ist, DHCP ausführt. Sie können diese Option auf der Registerkarte Erweitert im Richtlinienprofil aktivieren. Aktivieren Sie das Kontrollkästchen IPv4 DHCP Required. Wählen Sie unter den Einstellungen für die WLAN-Flex-Richtlinie die zuvor erstellte geteilte MAC-ACL aus der Dropdown-Liste "MAC-ACL aufteilen" aus. Klicken Sie auf Auf Gerät anwenden:

Cisco Catalys	st 9800-CL Wireless Cont	troller W	elcome admin 🛛 👫 🧒 🖺 🐇	000	Search APs and Clients Q
O Search Menu Items	Configuration * > Tags & Profi	Edit Policy Profile			×
Daekhaard	+ Add X Delete	Idle Threshold (bytes)	0	User Defined (Priva	ate) Network
	Status v Policy Profile Nam	Client Exclusion Timeout (sec)	60	Status	o
Monitoring >	O 🤄 Parameter and a	Guest LAN Session Timeout	0	Drop Unicast	o
Configuration	HomeOfficePolic	DHCP		Umbrella	
کې Administration		IPv4 DHCP Required	٥	Umbrella	Not Configured
C Licensing	□          ( orsuit-nouru-nn                      1         >>>         10	DHCP Server IP Address		Flex DHCP Option	
X Troubleshooting		Show more >>>		for DNS	
		AAA Policy	0	Redirect	
		NAC State	0	VLAN Central Switch	ing O
		Policy Name	default-aaa-policy x	Split MAC ACL	HomeOffice_ACU x v
		Accounting List	Search or Select 🔹	Air Time Fairness F	Policies
				2.4 GHz Policy	Search or Select
				5 GHz Policy	Search or Select
		Cancel			Update & Apply to Device

**Anmerkung:** Apple iOS-Clients benötigen Option 6 (DNS), um im DHCP-Angebot für Split-Tunneling konfiguriert zu werden.

### Zuordnen eines WLAN zu einem Richtlinienprofil

Schritt 1: Wählen Sie Konfiguration > Tags & Profile > Tags aus. Klicken Sie auf der Registerkarte Richtlinien auf Hinzufügen.

Schritt 2: Geben Sie den Namen der Tag-Richtlinie ein, und klicken Sie auf der Registerkarte WLAN-POLICY Maps (WLAN-POLICY-Karten) auf Hinzufügen.

Schritt 3: Wählen Sie das WLAN-Profil aus der Dropdown-Liste WLAN Profile (WLAN-Profil) aus, und wählen Sie das Richtlinienprofil aus der Dropdown-Liste Policy Profile (Richtlinienprofil) aus. Klicken Sie auf das Symbol Tick und dann auf Gerät anwenden.

Cisco Cisco	o Catalyst 9	9800-C	CL Wireless Contro	oller V	/elcome admin 🛛 🕋	• • •	0 2 Search APs a	nd Clients Q
Q. Search Menu Items	Cor	nfiguratio	in* > Tags & Profiles	s* > Tags				
Dashboard	Pol	licy	Site RF AP					
(C) Monitoring	-> <mark>-</mark>	+ Add	Add Policy Tag				×	
	>	Polk	Name*	HomeOfficePolicyTag				*
	>	C Locz	Description	Enter Description				
C Licensing		O RLA	V WLAN-POLI	CY Maps: 0				
X Troubleshooting		o defa	+ Add × D	elete			_	1 - 5 of 5 items
			WLAN Profile		<ul> <li>Policy Profile</li> </ul>		~	
			4 4 0 ⊨ ⇒	I I I I I I I I I I I I I I I I I I I		No	items to display	
			Map WLAN and P	olicy		_		
			WLAN Profile*	HomeOffice	Policy Profile*	HomeOffice	Policy	
			> RLAN-POLIC	CY Maps: 0				
			Cancel				Apply to Device	

#### Konfigurieren eines AP-Join-Profils und der Verknüpfung mit dem Site-Tag

Schritt 1: Navigieren Sie zu Konfiguration > Tags & Profile > AP Join (Konfiguration > Tags und Profile > AP Join), und klicken Sie auf Add (Hinzufügen). Geben Sie einen Namen ein. Optional können Sie SSH aktivieren, um die Fehlerbehebung zu ermöglichen, und diese später deaktivieren, wenn sie nicht benötigt wird.

Schritt 2: Wählen Sie Konfiguration > Tags & Profile > Tags aus. Klicken Sie auf der Registerkarte Standort auf Hinzufügen.

Schritt 3: Geben Sie den Namen des Standorts-Tags ein, deaktivieren Sie die Option Lokalen Standort aktivieren, und wählen Sie dann das AP-Join-Profil und das Flex-Profil (zuvor erstellt) aus den Dropdown-Listen aus. Dann auf Gerät anwenden.

Cisco Cisco Cata	alyst 9800-C	L Wireless Control	Welcome admin	* * 8 0 0	<b>2</b> Search APs and Clients <b>Q</b>	•
Q Search Meru Items	Configuratio	n * > Tags & Profiles '	Tags			
Dashboard	Policy	Site RF AP				
Monitoring	+ Add	Add Site Tag				×
	Site 1	Name*	HomeOficeSite			
	O defau	Description	Enter Description			
C Licensing		AP Join Profile	HomeOfficeAP •			4
X Troubleshooting		Flex Profile	HomeOffice_FlexPro			
		Fabric Control Plane N	•			
		Enable Local Site	•			
		Cancel			Apply to Dev	vice

### Anfügen eines Richtlinien-Tags und eines Site-Tags an einen Access Point

Option 1: Bei dieser Option müssen Sie jeweils einen Access Point konfigurieren. Gehen Sie zu Configuration > Wireless > Access Points. Wählen Sie den AP aus, den Sie zum Heimbüro verschieben möchten, und wählen Sie dann die Home Office-Tags aus. Klicken Sie auf Aktualisieren und auf Gerät anwenden:

Cisco Cisco Cat	talyst 9800-CL Wireless Contr	roller	Welcome admin		Search APs and Clients Q	•
Q, Search Menu Items	Configuration * > Wireless * >	Edit AP				×
Dashboard     Monitoring	All Access Points Number of AP(s): 1	Admin Status AP Mode Operation Status	ENABLED Cocal Cocal	Boot Version IOS Version Mini IOS Version	1.1.2.4 17.3.1.9 0.0.0.0	
Configuration	AP Name V Model	Fabric Status	Disabled	IP Config		
<ul> <li>Administration</li> <li>Licensing</li> </ul>	ah B  ≪ ≪ 1 ≫ 10 →	LED State LED Brightness Level	B v	CAPWAP Preferred Mode DHCP IPv4 Address	IPv4 192.168.100.29	
X Troubleshooting	> 5 GHz Radios	CleanAir <u>NSI Key</u>		Static IP (IPv4/IPv6)	0	- 1
	> 2.4 GHz Radios	Tags		Up Time	0 days 5 hrs 6	- 1
	> Dual-Band Radios	Changing Tags will lose associatio	cause the AP to momentarily n with the Controller.	Controller Association Late	mins 48 secs	
	> Country	Policy	HomeOfficePolicyTag +	ר ר		
	LSC Provision	Site RF	TiagoOfficeSite			
		Cancel		_	Update & Apply t	o Device

Es wird empfohlen, einen primären Controller zu konfigurieren, damit der Access Point die IP/Name des WLC kennt, die nach der Bereitstellung im Heimbüro erreicht werden soll. Sie können dies bearbeiten, indem Sie den Access Point direkt auf die Registerkarte "Hohe Verfügbarkeit" setzen:

				0.0240	23 A 10 A 10 A 10		0229226		
		Name	_	Man	agement IP A	ddress (IPv	4/IPv6)		
rimary Controller	eWLC	-9800-01		19	2.168.1.15				
econdary Controlle									
ertiary Controller									
P failover priority	Low								
			•						
			•						
			•						
			·						
			·						
			·						
			·						

Option 2: Mit dieser Option können Sie mehrere APs gleichzeitig konfigurieren. Navigieren Sie zu Configuration > Wireless Setup > Advanced > Tag APs. Wählen Sie die zuvor erstellten Tags aus, und klicken Sie auf Auf Gerät anwenden.

Cisco Catalyst 9800-CL Wireless Controller		Welcome admin
Q Search Meria terms	ranced	
Dashboard     Stan     Tags & Profiles	* Tag Al <sup>1</sup> / <sub>2</sub> Number of APs: 2 Selected Number of APs: 2	
Configuration > 0 WLAN Profile	AP AP Admin - AP Admin - AP Admin - Ap Admin - Mode Status	Operation - Hyperocot Status PolicyTag - Site Tag - Tag Location - Country - Method
Administration > Policy Profile	AP3800_E1.3EB8 AP38021. 0027.e336.5a60 Flex Enabled K9	Registered HomeOfficePolicyTag HomeOfficeSite of tag location PT Shared rad
C Licensing	AP9120_4C.E77C 09120AX0+ c064.e422.1780 Files Disacled	Registered HomeOfficePolicyTag TageOfficeSite eff-tag location US Dedicated
Troubleshooting	Tag APs Policy HameOfficePolicyTal • Site HameOfficePolicyTal • Changing AP Tag(s) will cause associated AP(s) to reco	Apply to Device

Die APs werden neu gestartet, und der WLC wird mit den neuen Einstellungen neu verbunden.

# Überprüfung

Sie können die Konfiguration über GUI oder CLI überprüfen. Dies ist die resultierende Konfiguration in der CLI:

```
1
ip access-list extended HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255 log
2 permit ip any any log
!
wireless profile flex HomeOffice_FlexProfile
acl-policy HomeOffice_ACL
office-extend
1
wireless profile policy HomeOfficePolicy
no central association
aaa-override
flex split-mac-acl HomeOffice_ACL
flex vlan-central-switching
ipv4 dhcp required
vlan default
no shutdown
1
wireless tag site HomeOficeSite
flex-profile HomeOffice_FlexProfile
no local-site
!
wireless tag policy HomeOfficePolicyTag
wlan HomeOffice policy HomeOfficePolicy
wlan HomeOffice 5 HomeOffice
security wpa psk set-key ascii 0 xxxxxx
no security wpa akm dot1x
security wpa akm psk
no shutdown
!
```

```
ap 70db.98el.3eb8
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
ap c4f7.d54c.e77c
policy-tag HomeOfficePolicyTag
site-tag HomeOfficeSite
!
```

#### AP-Konfiguration wird geprüft:

eWLC-9800-01#show ap name AP3800\_E1.3EB8 config general Cisco AP Name : AP3800\_E1.3EB8 Cisco AP Identifier : 0027.e336.5a60 . . . MAC Address : 70db.98e1.3eb8 IP Address Configuration : DHCP IP Address : 192.168.1.99 IP Netmask : 255.255.255.0 Gateway IP Address : 192.168.1.254 . . . SSH State : Enabled Cisco AP Location : default location Site Tag Name : HomeOficeSite RF Tag Name : default-rf-tag Policy Tag Name : HomeOfficePolicyTag AP join Profile : HomeOfficeAP Flex Profile : HomeOffice\_FlexProfile Primary Cisco Controller Name : eWLC-9800-01 Primary Cisco Controller IP Address : 192.168.1.15 . . . AP Mode : FlexConnect AP VLAN tagging state : Disabled AP VLAN tag : 0 CAPWAP Preferred mode : IPv4 CAPWAP UDP-Lite : Not Configured AP Submode : Not Configured Office Extend Mode : Enabled

Sie können eine direkte Verbindung zum Access Point herstellen und auch die Konfiguration überprüfen:

AP3800\_E1.3EB8#show ip access-lists Extended IP access list HomeOffice\_ACL 1 deny ip any 192.168.1.0 0.0.0.255 2 permit ip any any AP3800\_E1.3EB8#show capwap client detailrcb SLOT 0 Config SSID : HomeOffice Vlan Id : 0 Status : Enabled ... otherFlags : DHCP\_REQUIRED VLAN\_CENTRAL\_SW ... Profile Name : HomeOffice ...

```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800 E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name :
ssh status : Enabled
ApMode : FlexConnect
ApSubMode : Not Configured
Link-Encryption : Enabled
OfficeExtend AP : Enabled
Discovery Timer : 10
Heartbeat Timer : 30
. . .
```

Hier ein Beispiel für Paketerfassungen, die zeigen, dass der Datenverkehr lokal geschaltet wird. Dabei wurde ein "Ping" von einem Client mit IP 192.168.1.98 auf 8.8.8.8 und dann auf 192.168.1.254 getestet. Sie sehen, dass der ICMP, der die IP-Adresse der AP-IP-Adresse 192.168.1.99 erhält, an 8.8.8.8 gesendet wurde, da der Access Point NAT den Datenverkehr lokal verarbeitet. Es gibt kein icmp bis 192.168.1.254, da der Datenverkehr im DTLS-Tunnel verschlüsselt wird und nur Anwendungsdaten-Frames angezeigt werden.

*Ethernet_yellowCable													
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help													
🛋 🔳 🔬 💿 📙 🛅 🕱 🖆 🧣 👄 🕾 🗿 🖢 🚍 🔍 Q. Q. Q. X													
icmp													
No.		Delta	Source	Destination	Length I	Info				Ext Tag Number			
7*	825	0.000000	192.168.1.99	8.8.8	74 1	Echo	(ping) request	id=0x0001,	seq=13/3328				
+	831	0.018860	8.8.8.8	192.168.1.99	74 1	Echo	(ping) reply	id=0x0001,	seq=13/3328				
	916	0.991177	192.168.1.99	8.8.8	74 1	Echo	(ping) request	id=0x0001,	seq=14/3584				
	920	0.018004	8.8.8.8	192.168.1.99	74 8	Echo	(ping) reply	id=0x0001,	seq=14/3584				
	951	1.009921	192.168.1.99	8.8.8	74 8	Echo	(ping) request	id=0x0001,	seq=15/3840				
	954	0.017744	8.8.8.8	192.168.1.99	74 1	Echo	(ping) reply	id=0x0001,	seq=15/3840				
	1010	1.000264	192.168.1.99	8.8.8	74 8	Echo	(ping) request	id=0x0001,	seq=16/4096				
L	1011	0.018267	8.8.8	192.168.1.99	74 8	Echo	(ping) reply	id=0x0001,	seq=16/4096				

> Frame 825: 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: 8.8.8.8

> Internet Control Message Protocol

Anmerkung: Der lokal geswitchte Datenverkehr wird vom Access Point NATed verarbeitet, da das Client-Subnetz in normalen Szenarien zum Office-Netzwerk gehört und die lokalen Geräte im Heimbüro nicht wissen, wie das Client-Subnetz erreicht werden kann. Der AP übersetzt den Client-Datenverkehr mithilfe der AP-IP-Adresse, die sich im Subnetz des lokalen Heimbüros befindet.

Sie können auf die Access Point Office Extend-GUI zugreifen, einen Browser öffnen und die URL und die AP-IP-Adresse eingeben. Die Standardanmeldeinformationen sind admin/admin. Sie werden bei der ersten Anmeldung aufgefordert, sie zu ändern.



Nach der Anmeldung haben Sie Zugriff auf die GUI:

cisco	HOME CONFIGURATION	EVENT_LOG	NETWORK DIAGNOSTICS	HELP				Befresh Logout TELEWORKER
AP Info	Home: Summany							
SSID	Home. Summary							
	General Information							
Client	AP Name	AP3800 E1.3EB8						
	AP IP Address	192.168.1.99						
	AP Mode	FlexConnect						
	AP MAC Address	70:db:98:e1:3e:b8						
	AP Uptime	0 days, 0 hours, 52 minutes, 25 second		s				
	AP Software Version	17.3.1.9						
	WLC Info	[eWLC-9800-01][192.168.1.15]						
	CAPWAP Status	Run						
	WAN Gateway Status	Good						
	AP Statistics							
	Radio	Admin Status			Chan/BW	Tx Power	Pkts In/Out	
	2.4 GHz	Enabled		3	1/20MHz	14d8m	22338/145430	
	5 GHz	Enabled		1	36/40MHz	18dBm	0/0	
	LAN Port							
	Port No	Admin Stat	tus		Port Type	Link Status	Pkts In/Out	
	1	Disabled			Local	Blocked	0/0	
	2	Disabled			Local	Blocked	0/0	
	3	Disabled			Local	Blocked	0/0	
	4	Disabled		2	Local	Blocked	0/0	
	62010 - 2016 Circo Systems Inc. All tights reserved.							

Sie haben Zugriff auf typische Informationen in einem Office Extend AP, wie AP-Informationen, SSIDs und Clients verbunden:

ululu cisco	Номе	CONFIGURATION	EVENT_LOG	NETWORK DIAGNOSTICS	HELP			Refresh   Logout TELEWORKER
AP Info SSID	Associati	on						Show all
Client	Local Clien Client MAC	nts	Client IP		WLAN SSID	Radio/LAN	Association Time	Pkts In/Out
	Corporate Client MAC	Clients	Client IP		WLAN SSID	Radio/LAN	Association Time	Pkts In/Out
	98:22:EF:D4	:D1:09	192.168.1.98		HomeOffice	2.4GHz	00d:00h:00m:19s	46/2
	@2010 - 2016 Cisco Sy	stems inc. All rights reserved.						

## Zugehörige Dokumentation

FlexConnect auf Catalyst 9800 Wireless Controller

Split Tunneling für FlexConnect

Konfigurieren von OEAP und RLAN auf Catalyst 9800 WLC