

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

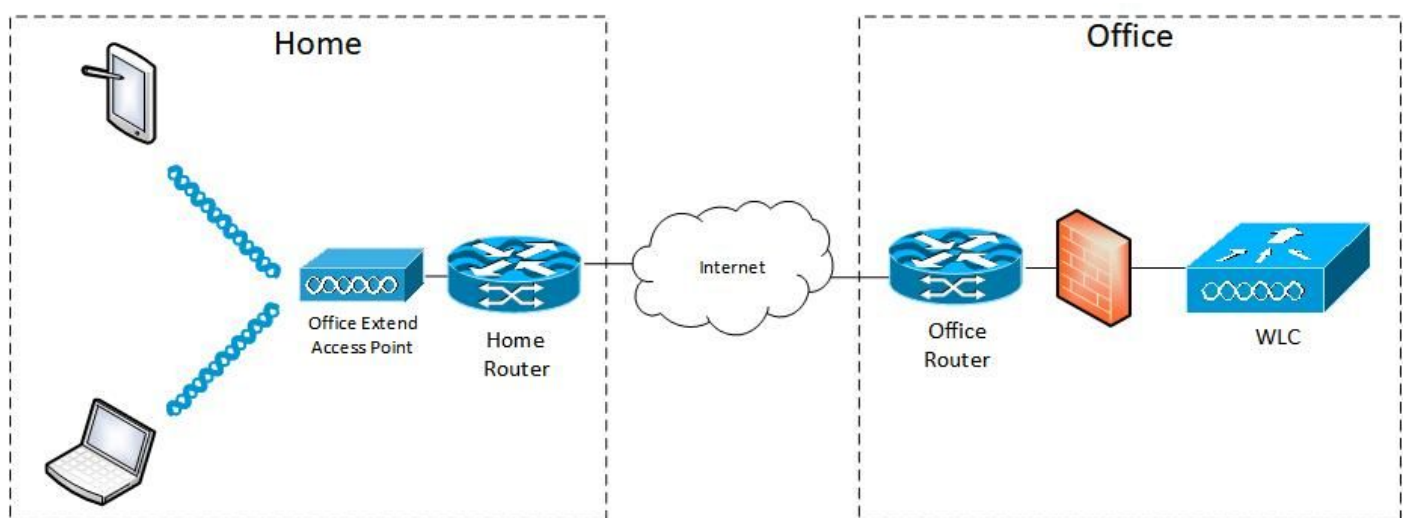
Um OEAP fornece comunicações seguras de uma WLC Cisco para um AP Cisco em um local remoto, para estender a WLAN corporativa pela Internet para a residência de um funcionário. A experiência do usuário no escritório doméstico é exatamente a mesma que seria no escritório corporativo. A criptografia DTLS (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

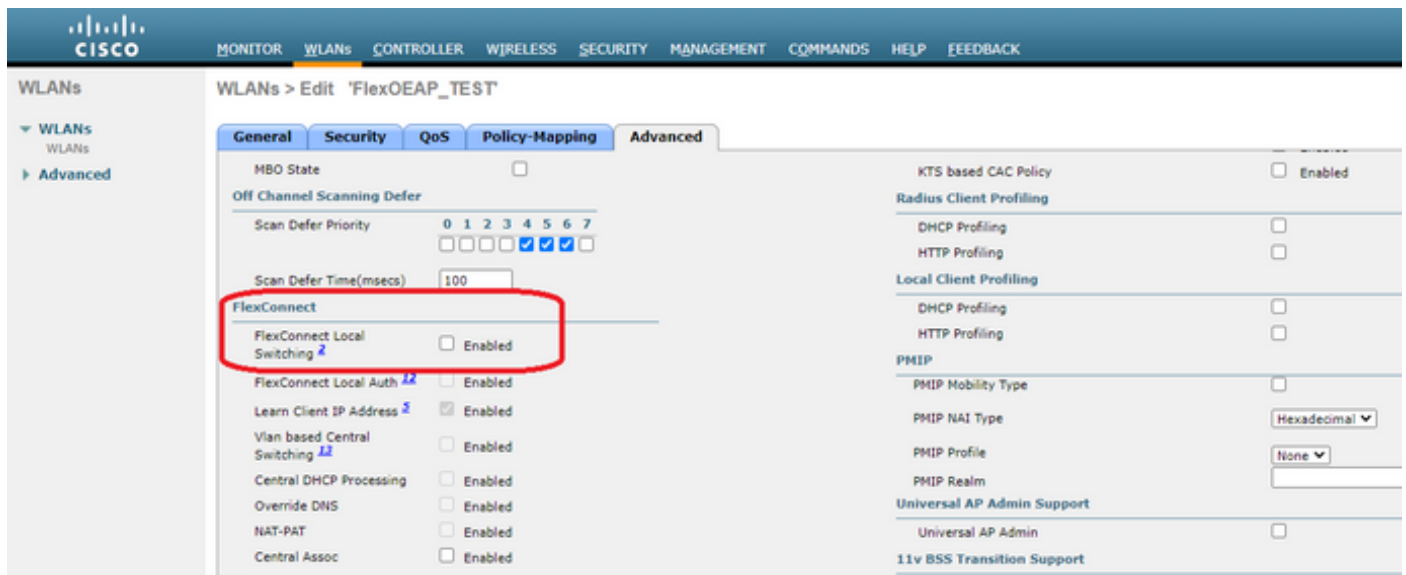
Diagrama de Rede



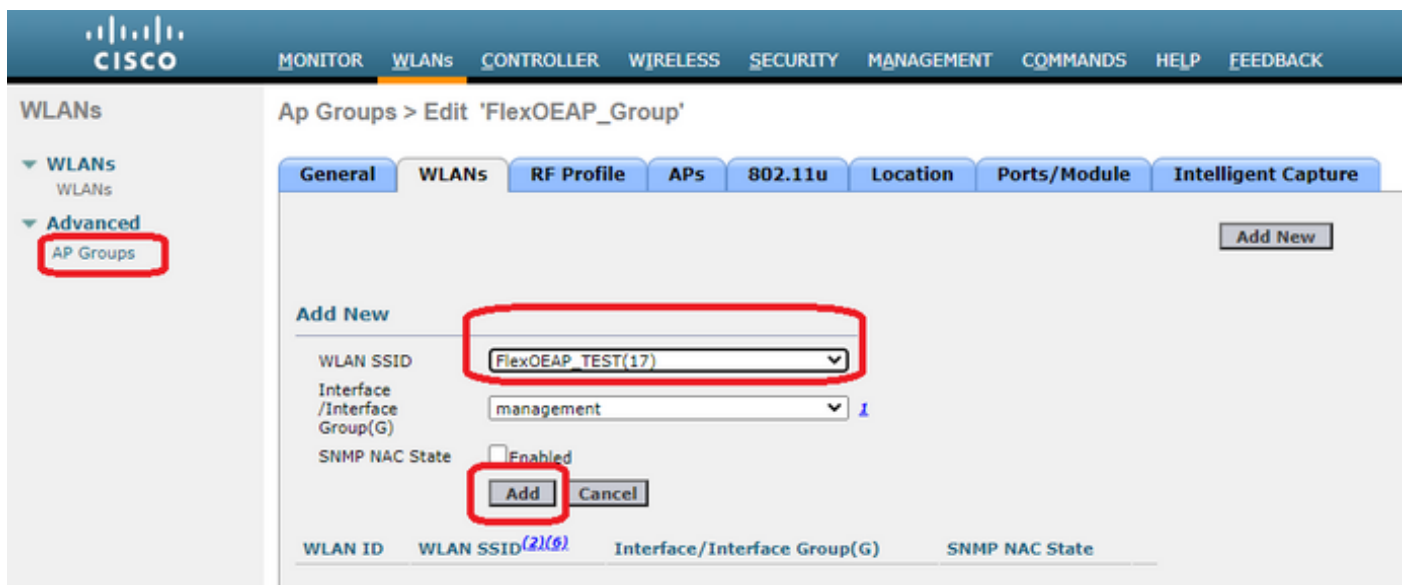
Configurações

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.



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.

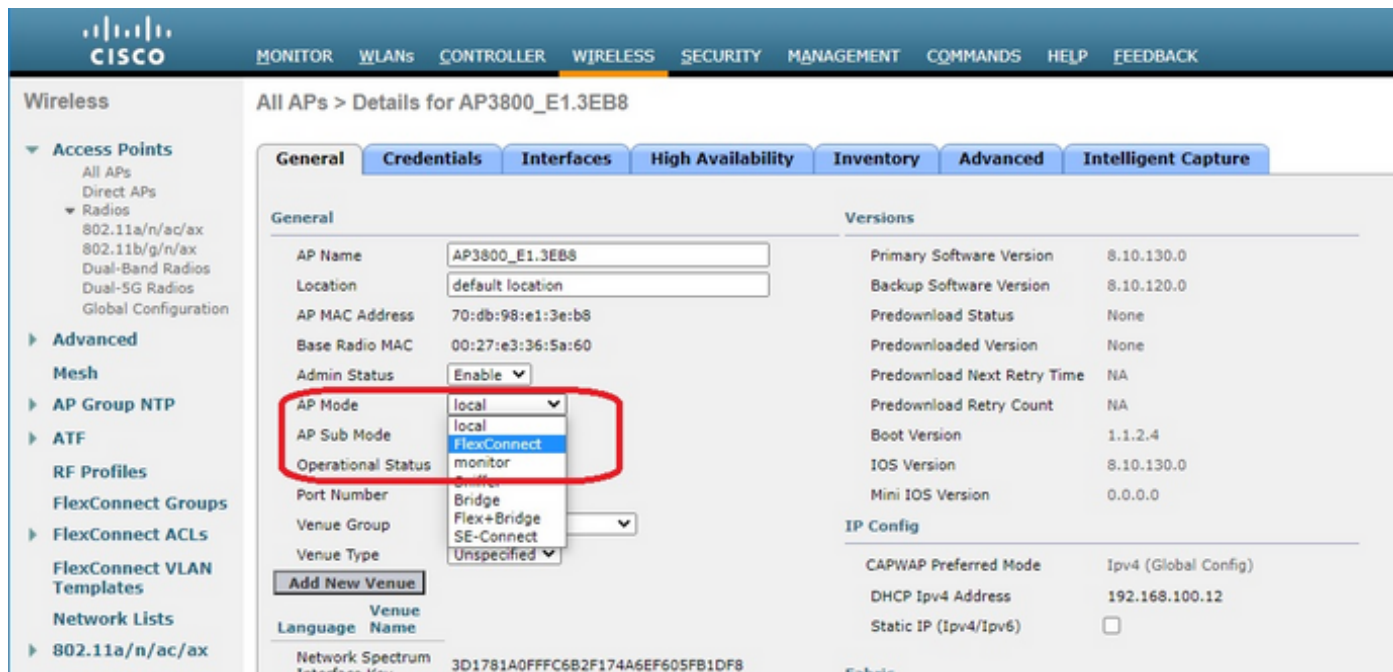


Configuração de AP

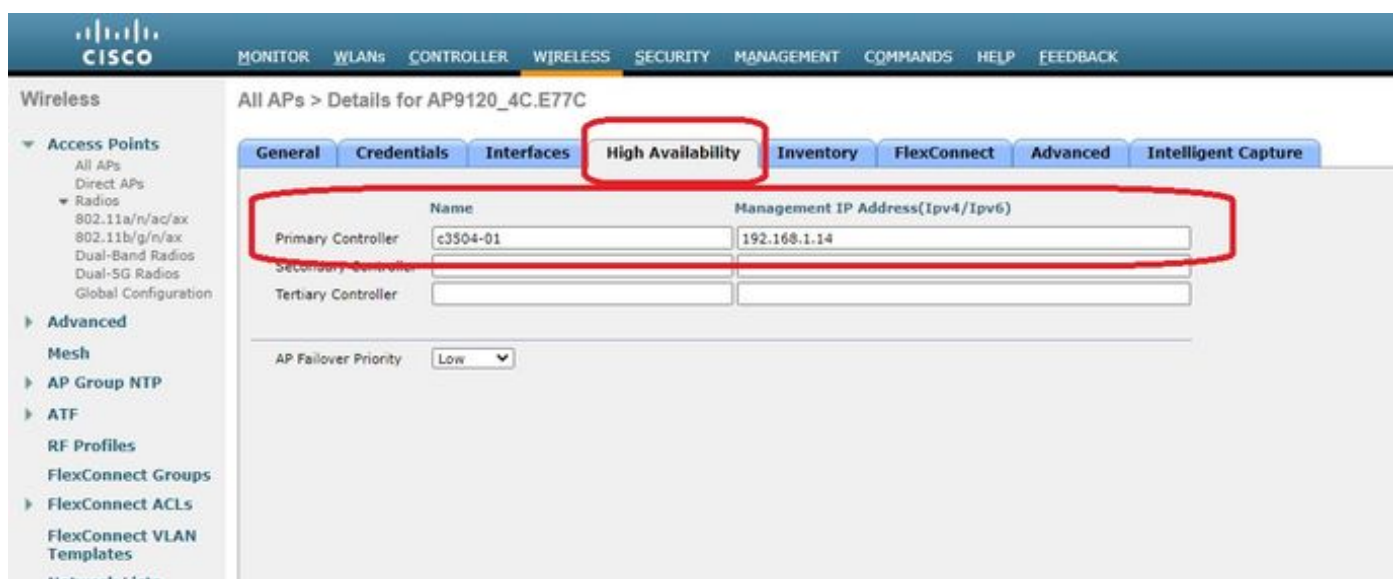
Depois que o AP estiver associado ao controlador no modo FlexConnect, você poderá configurá-

lo como um OEAP.

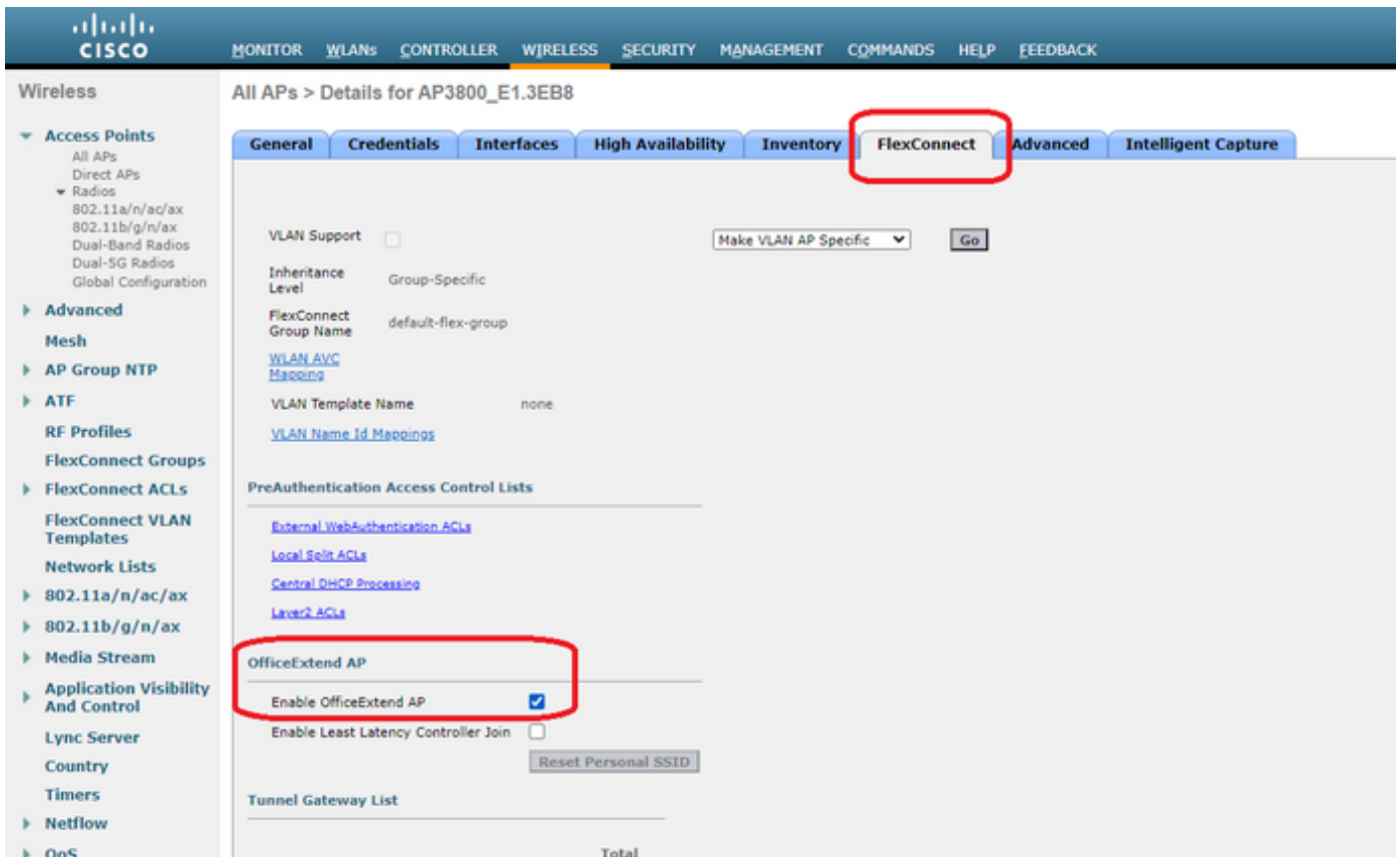
Etapa 1. Depois que o AP ingressar na WLC, altere o modo de AP para **FlexConnect** e clique em **Apply**.



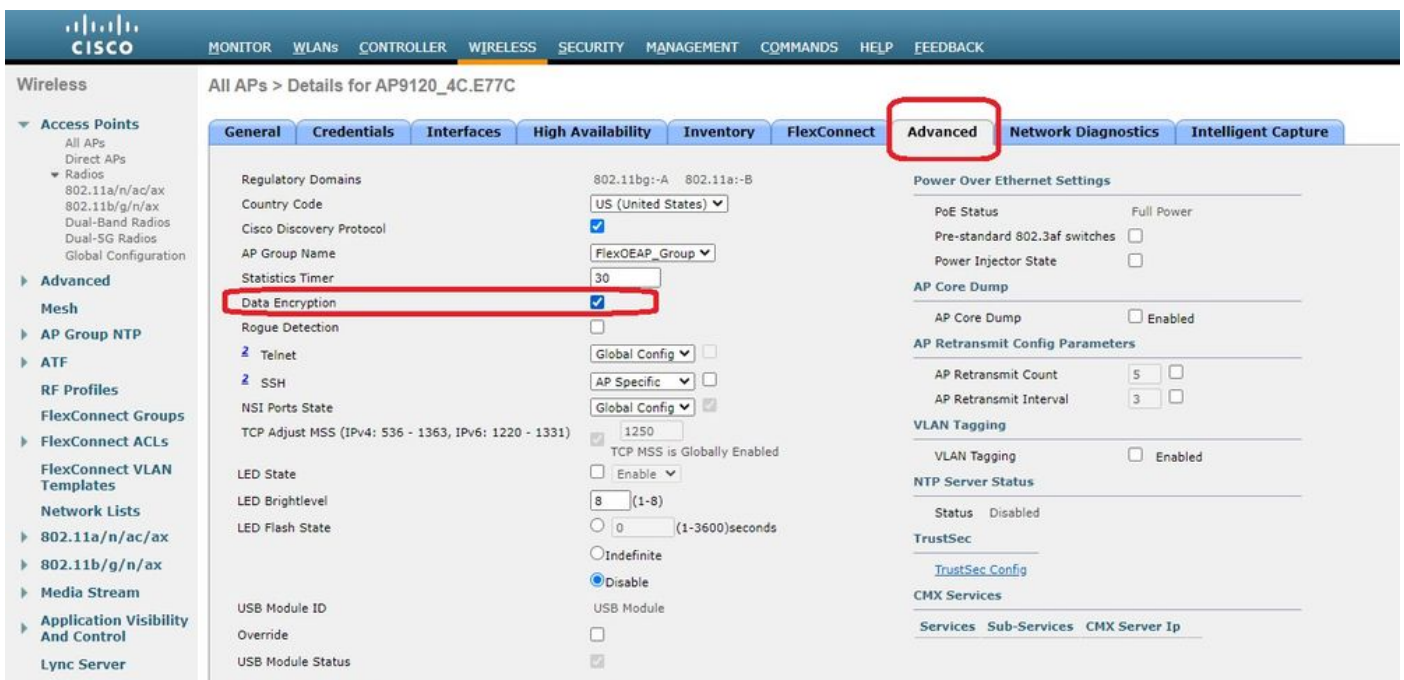
Etapa 2. Certifique-se de ter pelo menos uma WLC primária configurada na guia Alta disponibilidade:



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



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:



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.

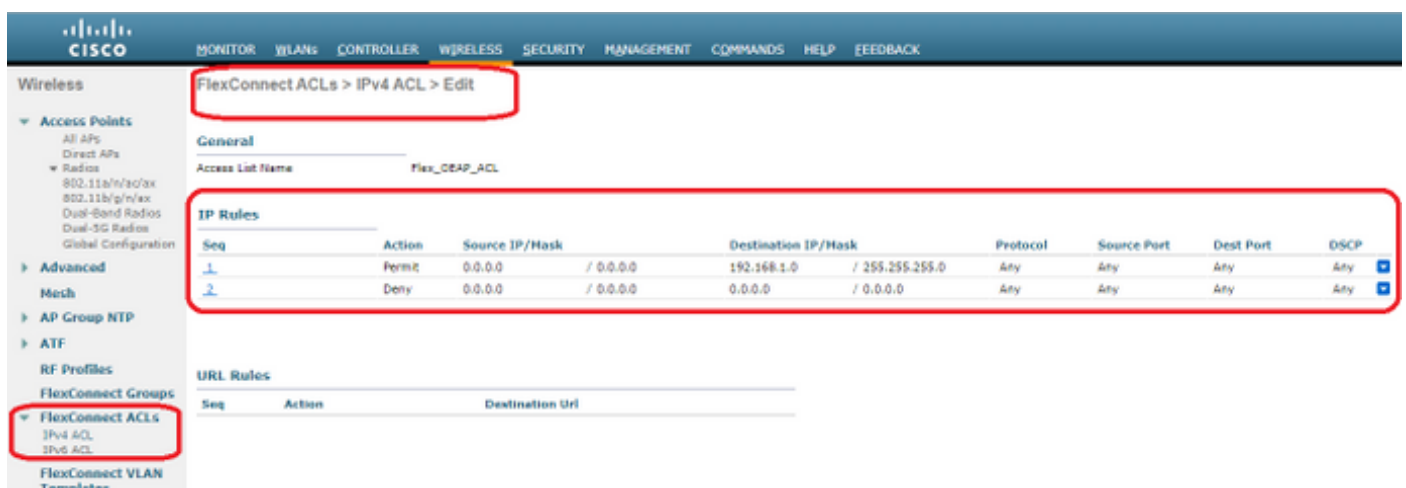
Etapa 3. Selecione **Aplicar**. Depois de selecionar Aplicar, o AP é recarregado.

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.

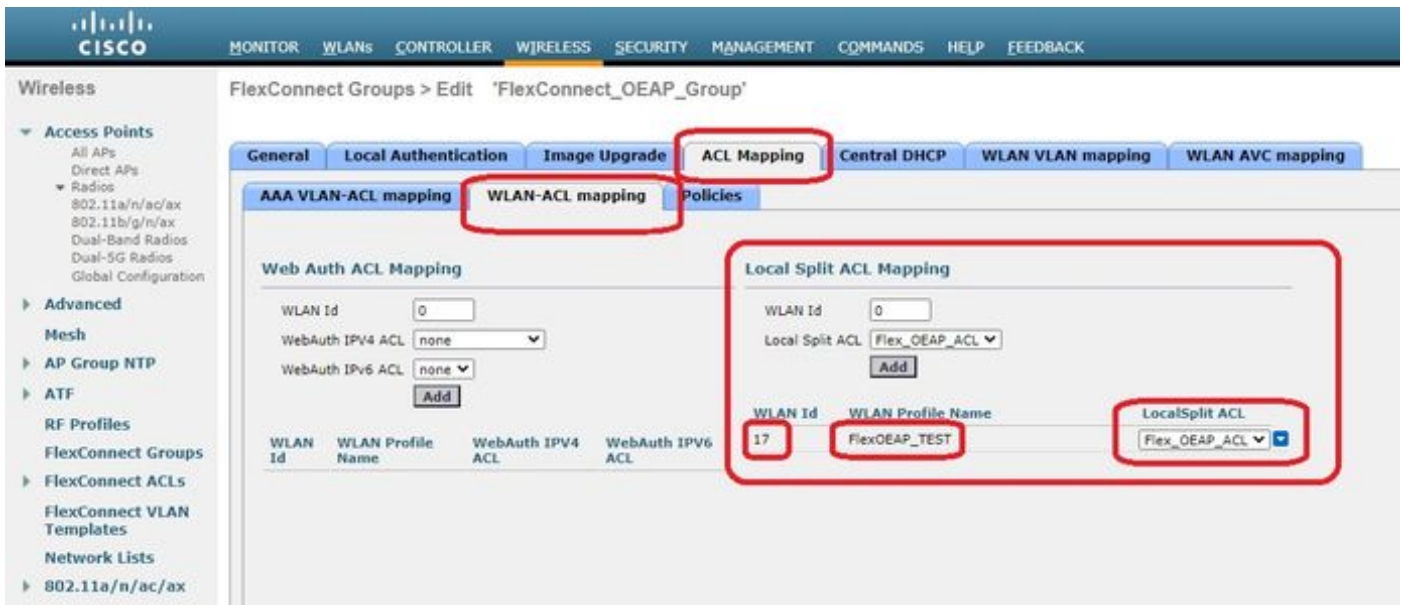


The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. The left sidebar shows the configuration tree with 'FlexConnect ACLs' selected. The main content area is titled 'FlexConnect ACLs > IPv4 ACL > Edit'. Under the 'General' tab, the 'Access List Name' is 'Flex_OEAP_ACL'. The 'IP Rules' section contains a table with two rules:

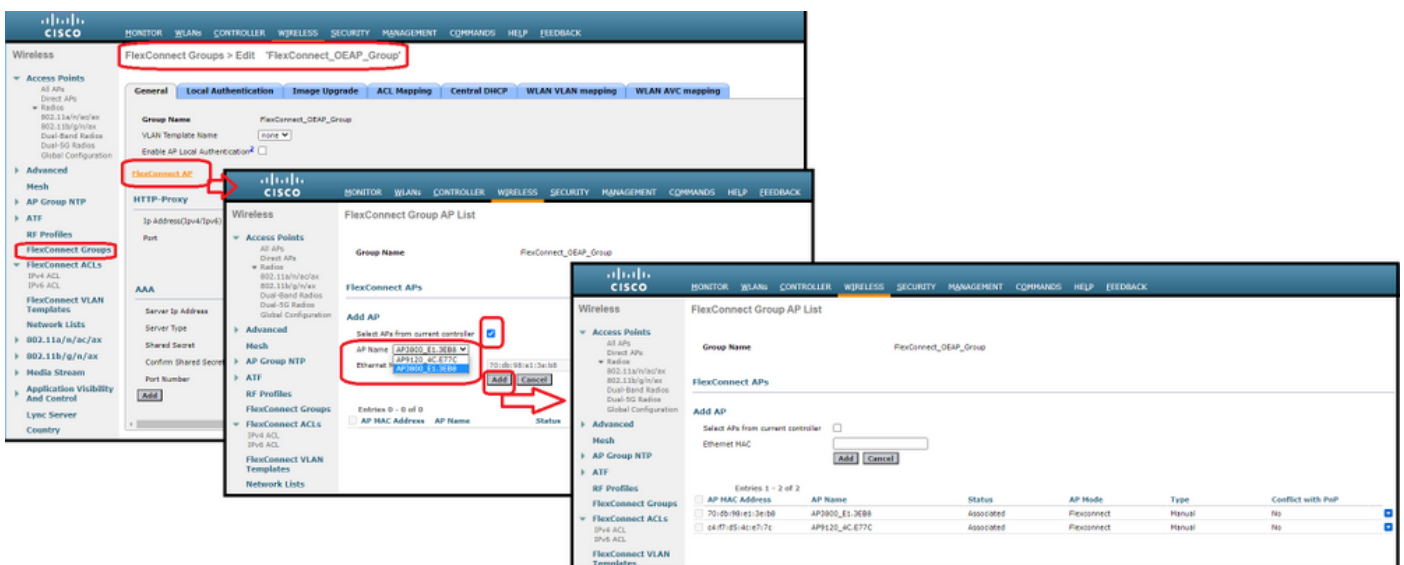
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	192.168.1.0 / 255.255.255.0	Any	Any	Any	Any
2	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any

The 'URL Rules' section is currently empty.

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**.



Passo 7. Adicione o AP ao grupo FlexConnect:



Verificar

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

```
(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 0.0.0.0/0.0.0.0 192.168.1.0/255.255.255.0 Any 0-65535 0-65535 Any Permit
2 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 Any 0-65535 0-65535 Any Deny
```

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-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
...
```

3. 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 :

Radius Retransmit Count..... 3 (default)

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 ID..... 436973636f0000000000000000000000

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_yellowCable

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Delta	Source	Destination	Length	Info	Ext Tag Number
20859	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	192.168.1.254	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

*Ethernet_yellowCable

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Delta	Source	Destination	Length	Info	Ext Tag Number
20859	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	192.168.1.254	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 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
```

```
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
```

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:

The image shows a Wireshark capture window titled "Capturing from Ethernet_yellowCable". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The main display area shows a list of captured packets, with the selected packet (No. 108) expanded to show its protocol layers.

No.	Delta	Source	Destination	Length	Info	Ext Tag Number	Payload Type	C
108	0.000000	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo (ping) request id=0x0001, seq=129/330...		MSDU	
109	0.000046	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=129/330...		MSDU	
127	1.000716	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo (ping) request id=0x0001, seq=130/332...		MSDU	
128	0.000266	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=130/332...		MSDU	
142	1.005703	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo (ping) request id=0x0001, seq=131/335...		MSDU	
143	0.000130	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=131/335...		MSDU	
165	1.008894	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo (ping) request id=0x0001, seq=132/337...		MSDU	
166	0.000133	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=132/337...		MSDU	

The expanded packet details for packet 108 are as follows:

- > 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