Configuration du protocole OEAP FlexConnect avec fractionnement de la transmission tunnel

Contenu

Introduction

Ce document décrit comment configurer un point d'accès intérieur (AP) en tant que mode OEAP (FlexConnect Office Extend AP) et comment activer la transmission tunnel partagée pour que vous puissiez définir quel trafic doit être commuté localement au bureau à domicile et quel trafic doit être commuté centralement au niveau du contrôleur de réseau local sans fil (WLC).

Contribué par Tiago Antunes, Nicolas Darchis Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

La configuration de ce document suppose que le WLC est déjà configuré dans une zone démilitarisée (DMZ) avec la traduction d'adresses de réseau (NAT) activée et que le point d'accès est capable de rejoindre le WLC depuis le bureau à domicile.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC avec la version du logiciel AireOS 8.10(130.0).
- Points d'accès Wave1 : 1700/2700/3700 .
- Points d'accès Wave2 : Gammes 1800/2800/3800/4800 et 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

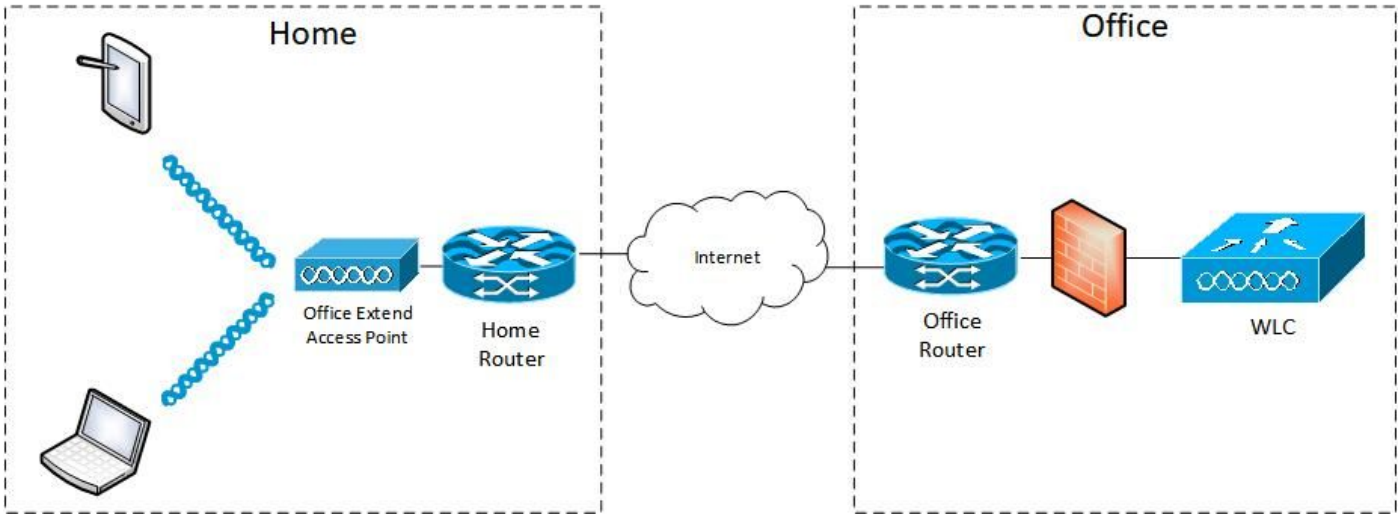
Un point d'accès OEAP fournit des communications sécurisées d'un WLC Cisco à un point d'accès Cisco sur un site distant, afin d'étendre le WLAN d'entreprise sur Internet à la résidence d'un employé. L'expérience de l'utilisateur au bureau à domicile est exactement la même que celle du bureau de l'entreprise. Le chiffrement DTLS (Datagram Transport Layer Security) entre le point d'accès et le contrôleur garantit que toutes les communications ont le niveau de sécurité le plus élevé. Tout point d'accès intérieur en mode FlexConnect peut agir en tant qu'OEAP.

Faits importants

- Les points d'accès OEAP Cisco sont conçus pour fonctionner derrière un routeur ou un autre périphérique de passerelle qui utilise NAT. La fonction NAT permet à un périphérique, tel qu'un routeur, d'agir en tant qu'agent entre Internet (public) et un réseau personnel (privé), ce qui permet à un groupe entier d'ordinateurs d'être représenté par une adresse IP unique. Il n'y a aucune limite au nombre de points d'accès OEAP Cisco que vous pouvez déployer derrière un périphérique NAT.
- Tous les modèles de points d'accès intérieurs pris en charge avec antenne intégrée peuvent être configurés en tant qu'OEAP, à l'exception des points d'accès AP-700I, AP-700W et AP802.
- Tous les points d'accès OEAP doivent se trouver dans le même groupe d'AP et ce groupe ne doit pas contenir plus de 15 LAN sans fil. Un contrôleur avec des points d'accès OEAP dans un groupe d'AP publie uniquement jusqu'à 15 WLAN sur chaque point d'accès OEAP connecté, car il réserve un WLAN pour l'identificateur SSID (Service Set Identifier) personnel.

Configuration

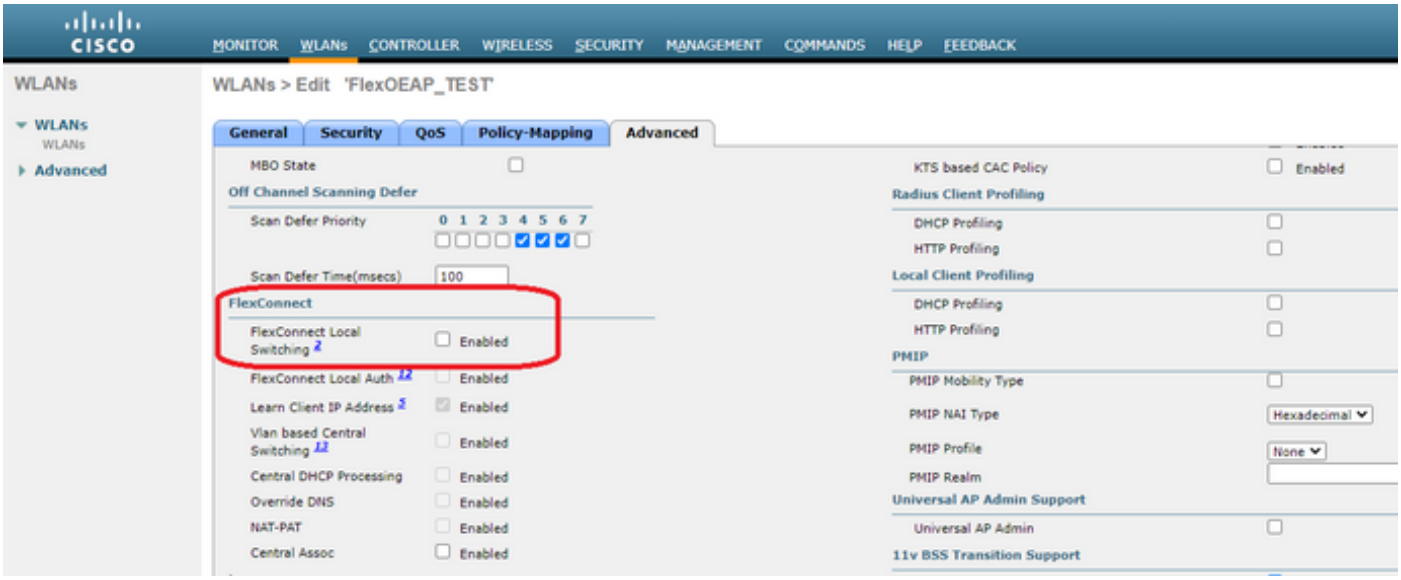
Diagramme du réseau



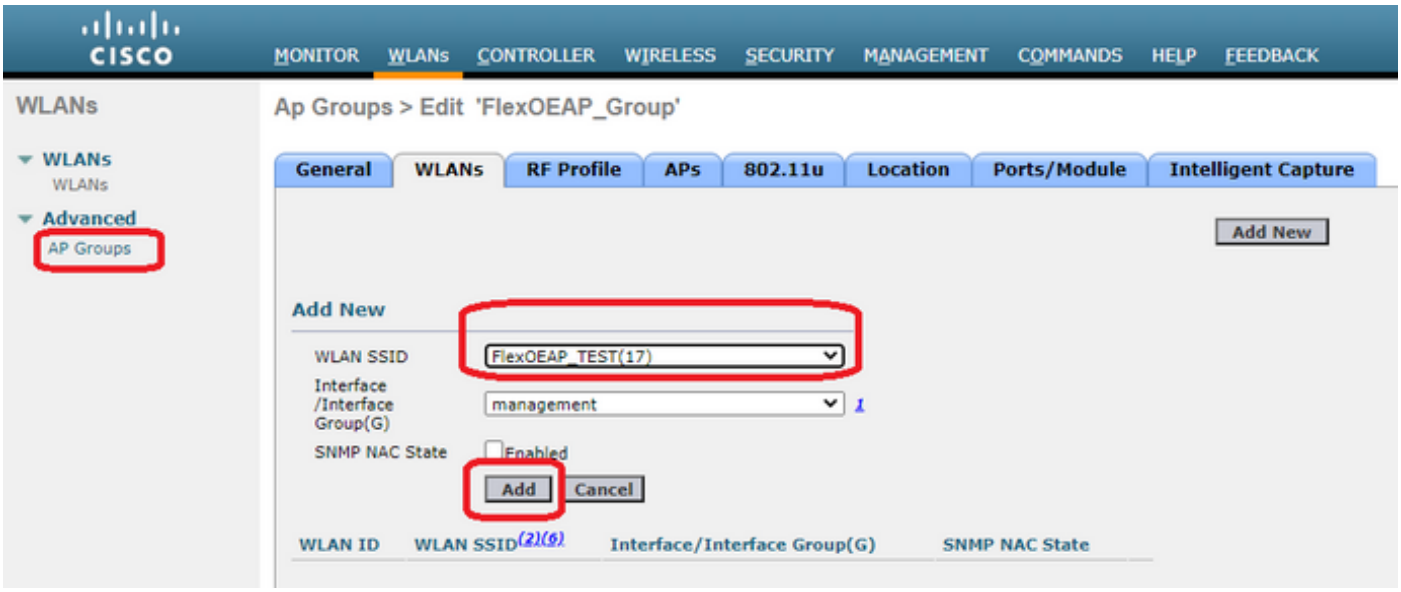
Configurations

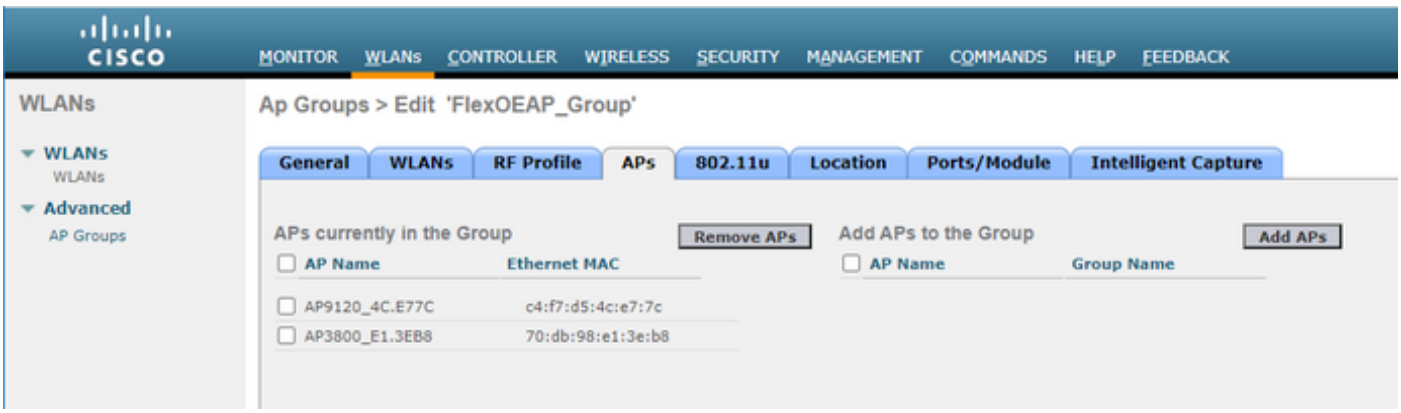
Configuration WLAN

Étape 1. Créez un WLAN à attribuer au groupe AP. Vous n'avez pas besoin d'activer l'option FlexConnect Local Switching pour ce WLAN.



Étape 2. Créez un groupe AP. Dans l'onglet **WLAN**, sélectionnez le SSID WLAN, puis cliquez sur **Add** pour ajouter le WLAN. Accédez à l'onglet **AP** et **ajoutez** le protocole OEAP FlexConnect.

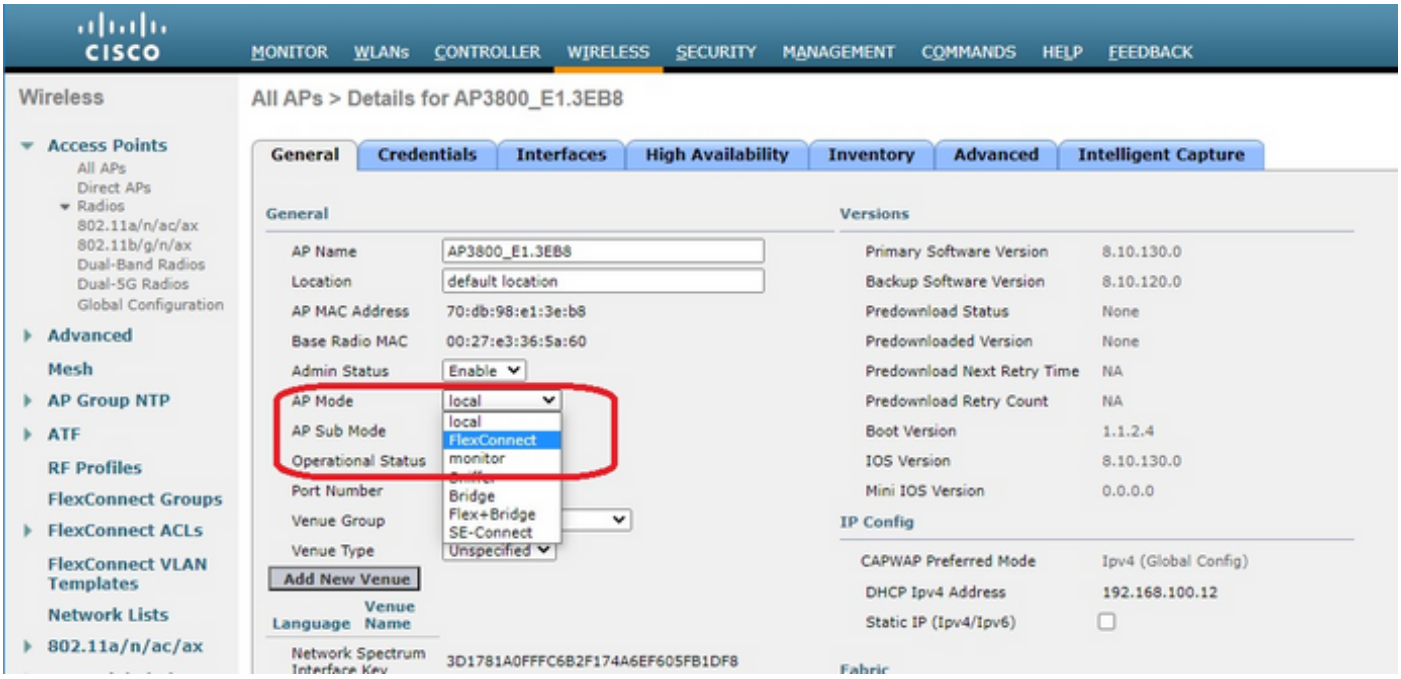




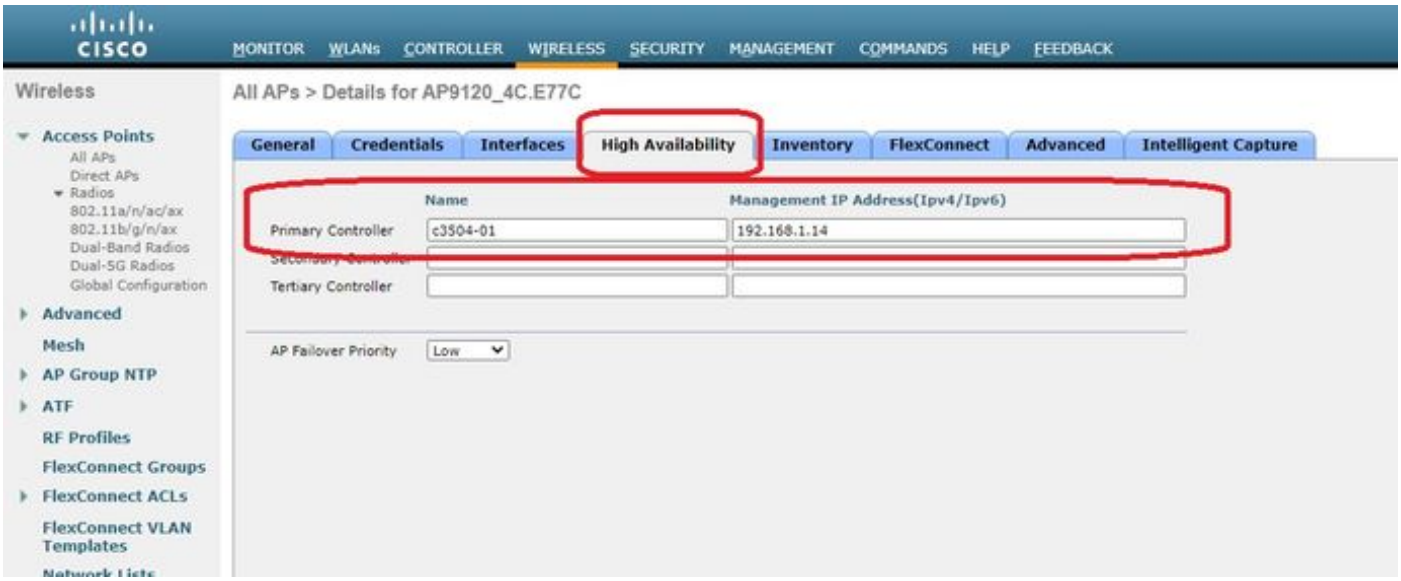
Configuration de point d'accès

Une fois que l'AP est associé au contrôleur en mode FlexConnect, vous pouvez le configurer en tant qu'OEAP.

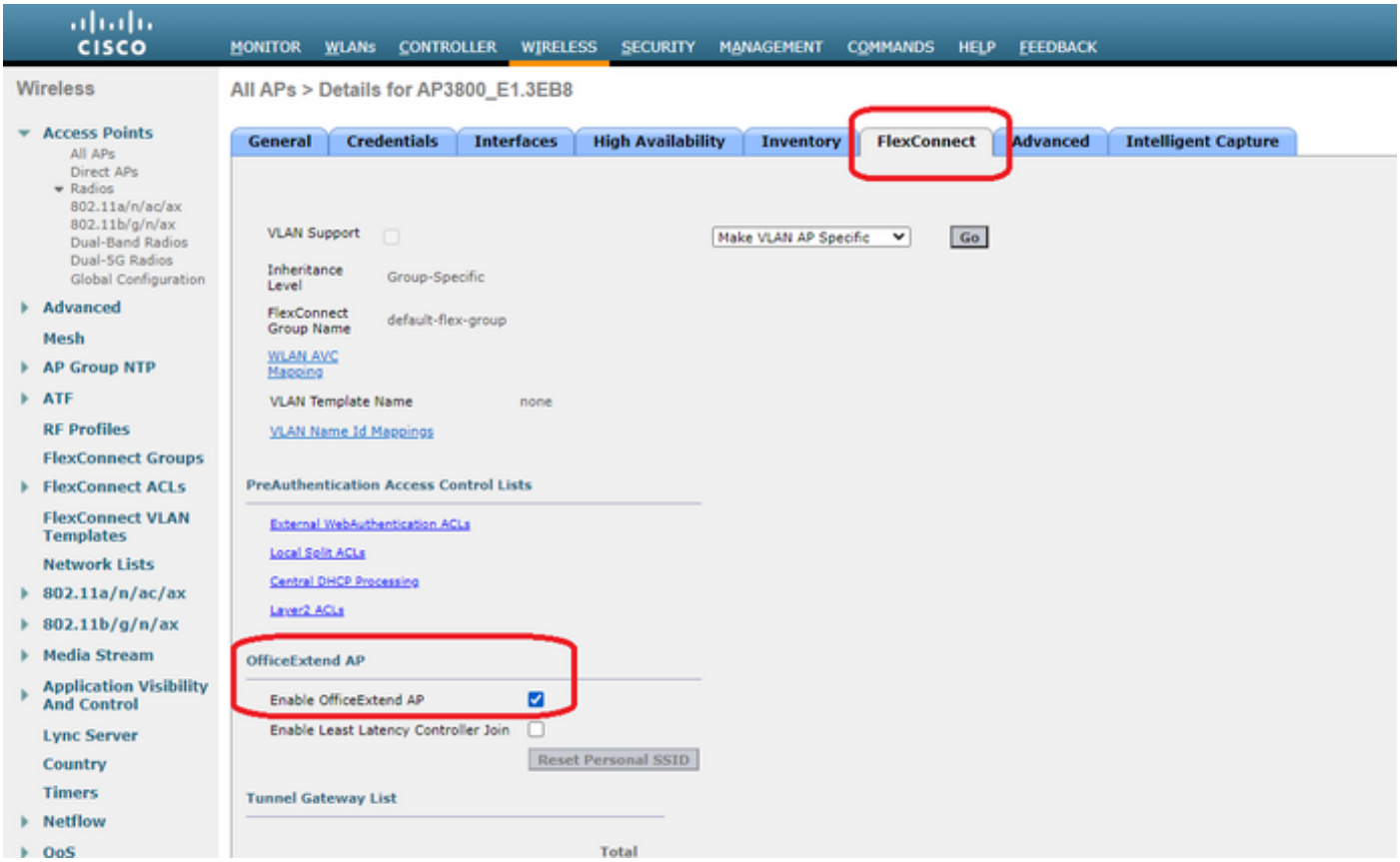
Étape 1. Une fois que l'AP a rejoint le WLC, changez le mode AP en **FlexConnect** et cliquez sur **Apply**.



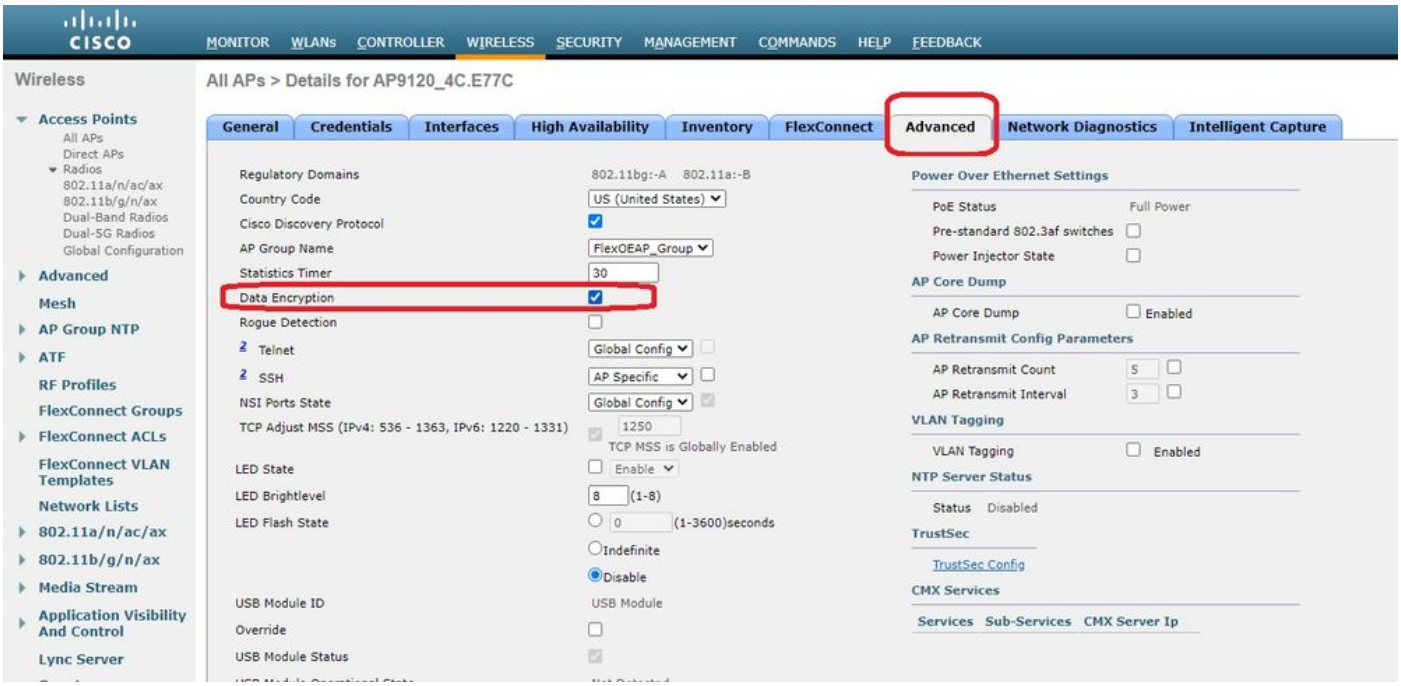
Étape 2. Assurez-vous qu'au moins un WLC principal est configuré dans l'onglet Haute disponibilité :



Étape 3. Accédez à l'onglet FlexConnect et cochez la case **Activer l'AP OfficeExtend**.



Le **chiffrement de données** DTLS est activé automatiquement lorsque vous activez le mode OfficeExtend pour un point d'accès. Cependant, vous pouvez activer ou désactiver le chiffrement de données DTLS pour un AP spécifique. Pour ce faire, cochez (activer) ou décochez (désactiver) la case **Data Encryption** sur Tous les AP > Détails pour [AP sélectionné] > onglet Avancé :



Note: L'accès Telnet et SSH est désactivé automatiquement lorsque vous activez le mode OfficeExtend pour un point d'accès. Cependant, vous pouvez activer ou désactiver l'accès Telnet ou SSH pour un AP spécifique. Pour ce faire, cochez (activer) ou décochez (désactiver) la case Telnet ou SSH dans l'onglet Tous les AP > Détails pour [AP sélectionné] > Avancé.

Note: La latence de liaison est activée automatiquement lorsque vous activez le mode OfficeExtend pour un point d'accès. Cependant, vous pouvez activer ou désactiver la latence de liaison pour un AP spécifique. Pour ce faire, cochez (activer) ou décochez (désactiver) la case Activer la latence de liaison dans l'onglet Tous les AP > Détails pour [AP sélectionné] > Avancé.

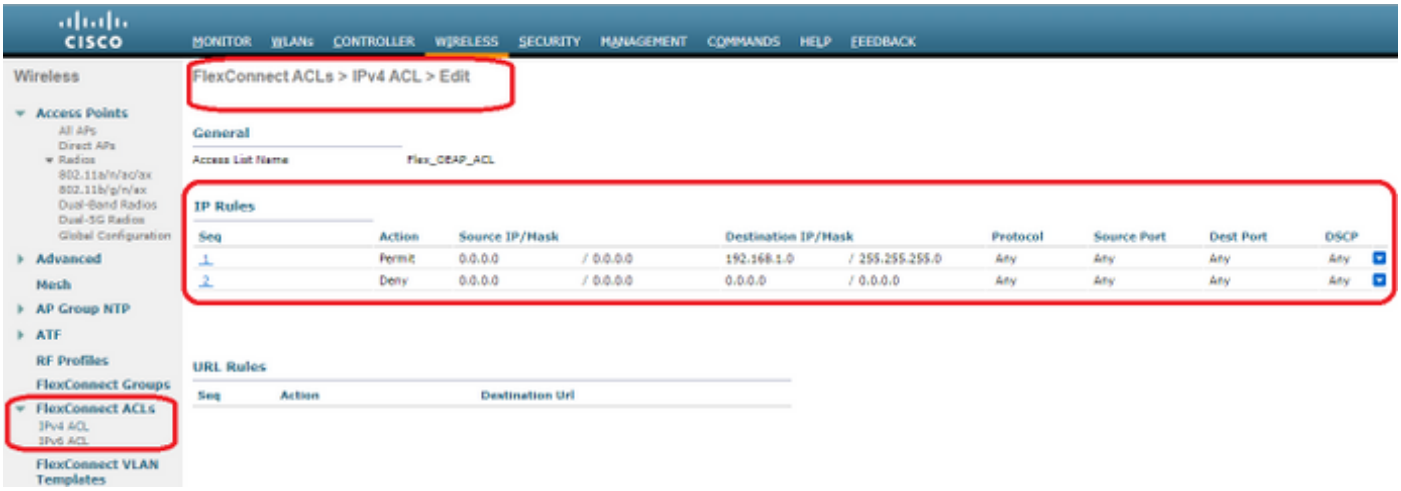
Étape 3. Sélectionnez **Appliquer**. Après avoir sélectionné Appliquer, l'AP se recharge.

Étape 4. Après que l'AP se connecte au WLC, l'AP est en mode OEAP.

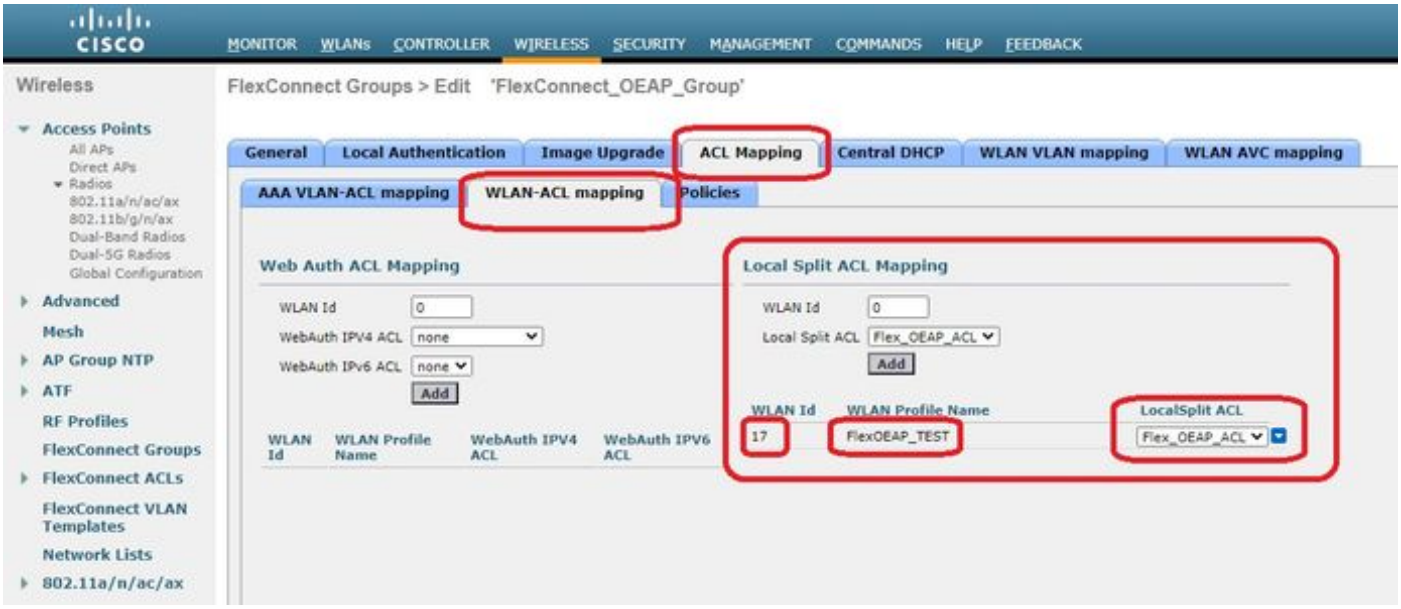
Note: Nous vous recommandons de configurer la sécurité de jonction AP (généralement définie sous Stratégies AP) de sorte que seuls les AP autorisés puissent rejoindre le WLC. Vous pouvez également utiliser le provisionnement des points d'accès LSC (Certificat significatif localement).

Étape 5. Créez une liste de contrôle d'accès (ACL) FlexConnect pour définir le trafic qui sera commuté centralement (Deny) et localement (Permit).

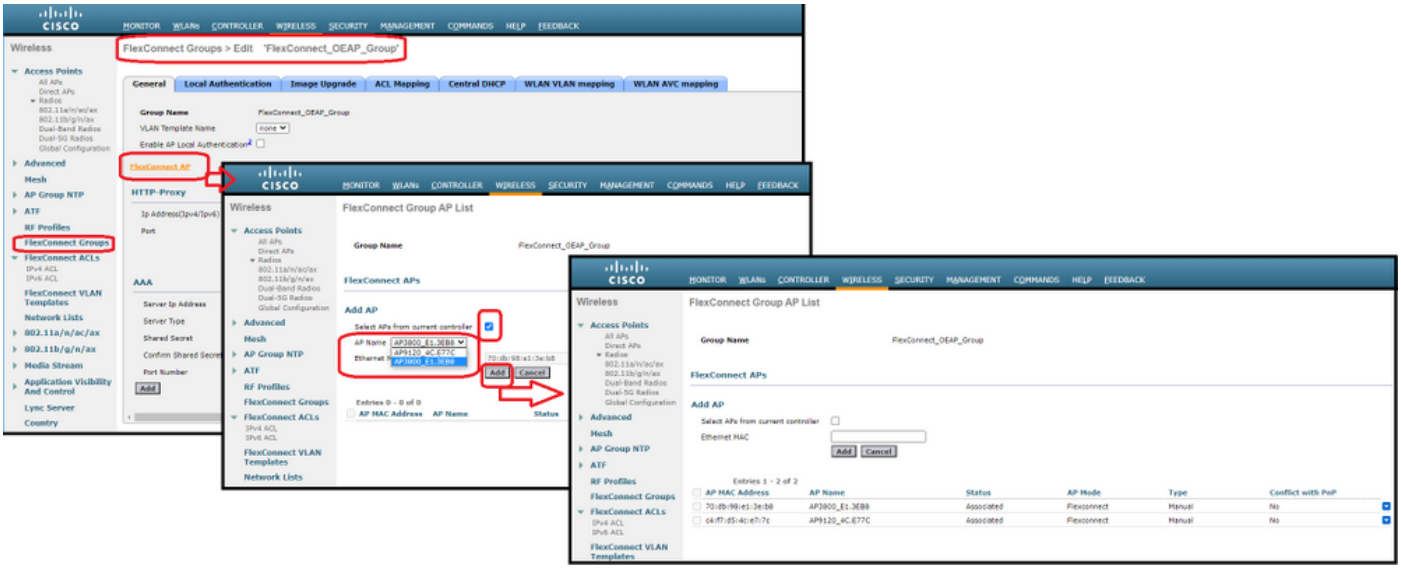
Ici, vous avez l'objectif de commuter localement tout le trafic vers le sous-réseau 192.168.1.0/24.



Étape 6. Créez un groupe FlexConnect, accédez à **Mappage ACL**, puis accédez à **Mappage ACL WLAN**. Sous « Local Split ACL Mapping », saisissez l'ID WLAN et choisissez la liste de contrôle d'accès FlexConnect. Cliquez ensuite sur **Ajouter.**



Étape 7. **Ajoutez** l'AP au groupe FlexConnect :



Vérification

1. Vérifiez l'état et la définition de la liste de contrôle d'accès 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. Vérifiez que la commutation locale FlexConnect est désactivée :

```
(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. Vérifiez la configuration du groupe FlexConnect :

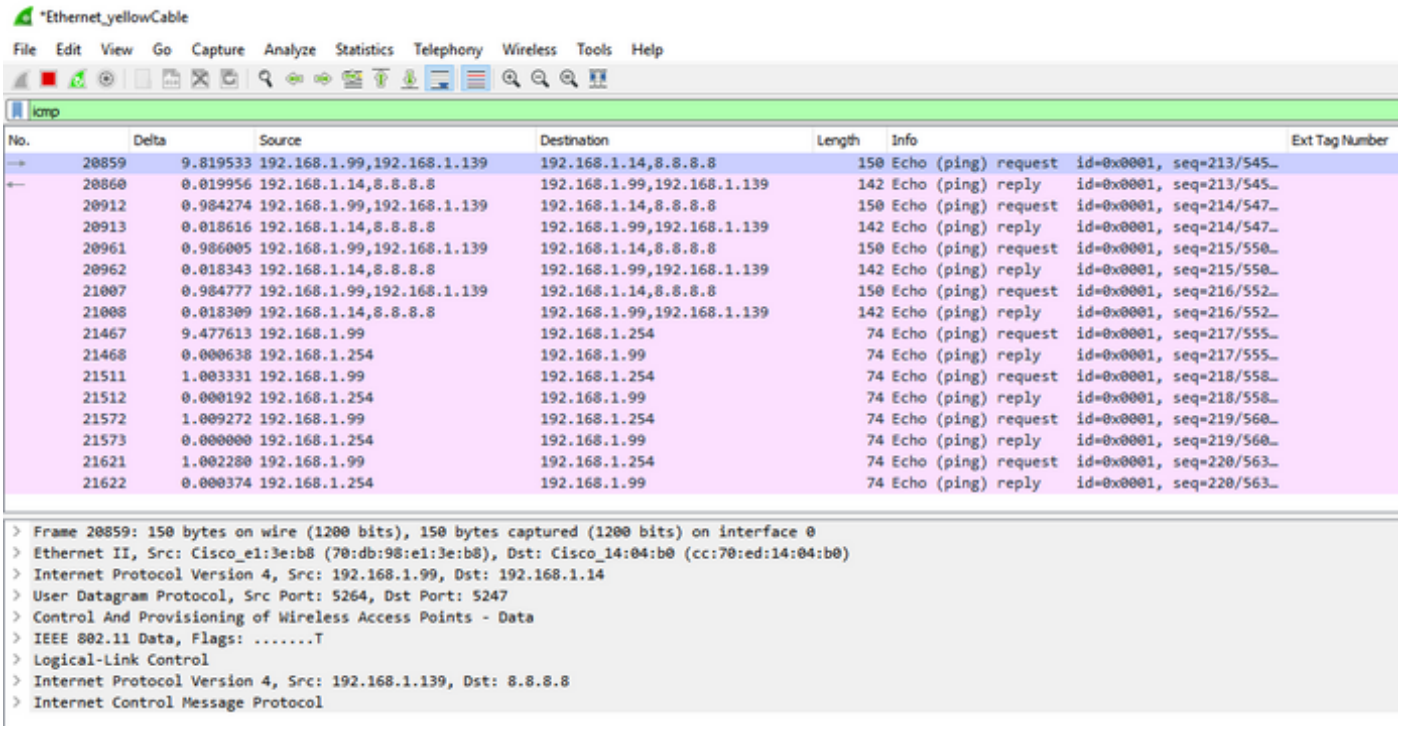
```
(c3504-01) >show flexconnect group summary

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
```

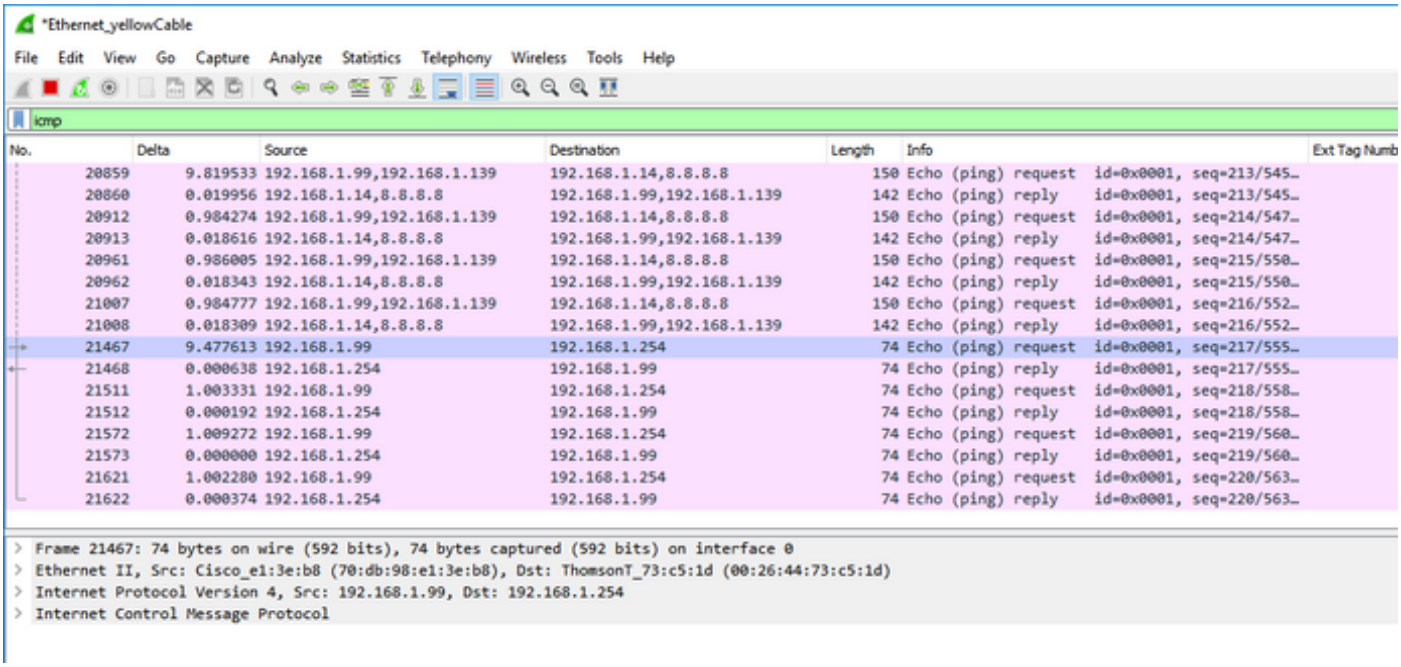
```
Group Radius Servers Settings:
Type Server Address Port
------------ --------------- -------
Primary Unconfigured Unconfigured
Secondary Unconfigured Unconfigured

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..... 436973636f00000000000000000000000
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
```

Vous pouvez capturer le trafic au niveau de l'interface AP afin de vérifier que le trafic est fractionné au niveau de l'AP.

> **Conseil** : à des fins de dépannage, vous pouvez désactiver le chiffrement DTLS afin de voir le trafic de données encapsulé dans le capwap.

Cet exemple de capture de paquets montre le trafic de données qui correspond aux instructions « deny » de la liste de contrôle d'accès dirigées vers le WLC, et le trafic de données qui correspond aux instructions « permit » de la liste de contrôle d'accès commutées localement sur le point d'accès :





> **Note**: Dans des scénarios normaux, le point d'accès traduit les adresses réseau pour le trafic commuté localement parce que le sous-réseau du client appartient au réseau du bureau et que les périphériques locaux du bureau à domicile ne savent pas comment atteindre le sous-réseau du client. Le point d'accès utilise l'adresse IP définie dans le sous-réseau du bureau à domicile local pour traduire le trafic client.

Afin de vérifier que l'AP a effectué la NAT, vous pouvez vous connecter au terminal AP et émettre la commande ***show ip nat translations***. Exemple :

```
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
```

Si vous supprimez la transmission tunnel partagée, tout le trafic est commuté de façon centralisée au niveau du WLC. Cet exemple montre le protocole ICMP (Internet Control Message Protocol) vers la destination 192.168.1.2, à l'intérieur du tunnel capwap :