# Exemple de configuration d'un filtre ACL de point d'accès

## Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
**[Informations générales](#)**
[Configurez](#)
[Filtres utilisant des listes d'accès standard](#)
[Filtres utilisant des listes d'accès étendues](#)
[Filtres utilisant des listes de contrôle d'accès basées sur MAC](#)
[Filtres utilisant des listes de contrôle d'accès basées sur l'heure](#)
[Vérifiez](#)
[Dépannez](#)
**[Informations connexes](#)**

# Introduction

Ce document explique comment configurer les filtres basés sur des listes de contrôle d'accès (ACL) sur des points d'accès Cisco (AP) Aironet à l'aide de l'interface de ligne de commande (CLI).

# Conditions préalables

## Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration d'une connexion sans fil à l'aide d'un AP Aironet et d'un adaptateur client Aironet 802.11 a/b/g
- ACLs

## Composants utilisés

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

- Point d'accès (AP) de la gamme Aironet 1200 qui exécute le logiciel Cisco IOS® Version 12.3(7)JA1
- Adaptateur client Aironet 802.11a/b/g
- Aironet Desktop Utility (ADU), version 2.5

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

## Informations générales

Vous pouvez utiliser des filtres sur l'application pour effectuer ces tâches :

- Restreindre l'accès au réseau sans fil LAN (WLAN)
- Fournir une couche supplémentaire de sécurité sans fil

Vous pouvez utiliser différents types de filtres pour filtrer le trafic en fonction :

- de protocoles spécifiques ;
- de l'adresse MAC du périphérique client ;
- de l'adresse IP du périphérique client.

Vous pouvez également permettre à des filtres de restreindre le trafic depuis des utilisateurs sur le réseau local câblé. Les filtres d'adresse IP et d'adresse MAC permettent ou rejettent le transfert des paquets de monodiffusion et de multidiffusion qui sont envoyés vers ou depuis des adresses IP ou MAC spécifiques.

Les filtres basés sur des protocoles fournissent une façon plus précise de restreindre l'accès aux protocoles spécifiques par les interfaces Ethernet et radios de l'AP. Vous pouvez utiliser l'une ou l'autre de ces méthodes pour configurer les filtres sur les AP :

- GUI Web
- CLI

Ce document explique comment utiliser les filtres de liste de contrôle d'accès par la CLI. Pour obtenir des informations sur la façon de configurer des filtres par l'interface graphique, consultez Configuration des filtres.

Vous pouvez utiliser la CLI pour configurer ces types de filtres basés sur ACL sur l'AP :

- Filtres qui utilisent des listes de contrôle d'accès standard
- Filtres qui utilisent des listes de contrôle d'accès étendues
- Filtres qui utilisent des listes de contrôle d'accès d'adresse MAC

**Remarque:** Le nombre d'entrées de routage permises sur une ACL est limité par le processeur de l'AP. S'il faut ajouter un grand nombre d'entrées de routage à une ACL, par exemple en filtrant une liste d'adresses MAC pour les clients, utilisez un commutateur dans le réseau qui peut effectuer la tâche.

# Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Toutes les configurations dans ce document supposent qu'une connexion sans fil est déjà établie. Ce document se focalise seulement sur la façon d'utiliser la CLI afin de configurer des filtres. Si vous n'avez pas une connexion sans fil de base, consultez la section Exemple de configuration de connexion LAN sans fil de base.

## Filtres utilisant des listes d'accès standard

Vous pouvez utiliser des listes de contrôle d'accès standard pour autoriser ou rejeter l'entrée de périphériques clients dans le réseau WLAN basé sur l'adresse IP du client. Les listes de contrôle d'accès standard comparent l'adresse source des paquets IP aux adresses qui sont configurées dans la liste de contrôle d'accès afin de contrôler le trafic. Ce type de liste de contrôle d'accès peut être désigné comme étant basé sur l'adresse IP source.

La syntaxe des commandes applicables aux listes de contrôle d'accès standard est la suivante : **access-list access-list-number {permit | deny} {host ip-address |** *source-ip source-wildcard* **| quels}**.

Dans la version 12.3(7)JA de Cisco IOS®, le numéro de la liste de contrôle d'accès peut être n'importe quel numéro de 1 à 99. Les listes de contrôle d'accès standard peuvent également utiliser une plage étendue de 1300 à 1999. Ces numéros supplémentaires sont des listes de contrôle d'accès IP étendues.

Quand une liste de contrôle d'accès standard est configurée pour refuser l'accès à un client, le client s'associe toujours à l'AP. Cependant, il n'y a aucune communication de données entre l'AP et le client.

Cet exemple montre une liste de contrôle d'accès standard qui est configurée pour filtrer l'adresse IP 10.0.0.2 du client depuis l'interface sans fil (interface radio0). L'adresse IP de l'AP est 10.0.0.1.

Après cela, le client avec l'adresse IP 10.0.0.2 ne peut pas envoyer ou recevoir de données par le réseau WLAN même s'il est associé à l'AP.

Effectuez ces étapes afin de créer une liste de contrôle d'accès standard par la CLI :

1. Connectez-vous à l'AP par la CLI.Utilisez le port de console ou Telnet afin d'accéder à l'ACL par l'interface Ethernet ou l'interface sans fil.
2. Passez en mode de configuration globale sur l'AP :`AP#configure terminal`
3. Exécutez ces commandes afin de créer la liste de contrôle d'accès standard :`AP<config>#access-list 25 deny host 10.0.0.2 !--- Create a standard ACL 25 to deny access to the !--- client with IP address 10.0.0.2. AP<config>#access-list 25 permit any !--- Allow all other hosts to access the network.`
4. Exécutez ces commandes afin d'appliquer cette ACL à l'interface radio :`AP<config>#interface Dot11Radio 0 AP<config-if>#ip access-group 25 in !--- Apply the standard ACL to the radio interface 0.`

Vous pouvez également créer une ACL standard nommée (NACL). La NACL emploie un nom au lieu d'un numéro pour définir l'ACL.

```
 AP#configure terminal AP<config>#ip access-list standard name AP<config>#permit | deny {host ip-address | source-ip [source-wildcard] | any} log
```

Exécutez ces commandes afin d'utiliser des NACL standard pour refuser l'accès de l'hôte 10.0.0.2 au réseau WLAN :

```
AP#configure terminal AP<config>#ip access-list standard TEST !--- Create a standard NACL TEST. AP<config-std-nacl>#deny host 10.0.0.2 !--- Disallow the client with IP address 10.0.0.2 !--- access to the network. AP<config-std-nacl>#permit any !--- Allow all other hosts to access the network. AP<config-std-nacl>#exit !--- Exit to global configuration mode. AP<config>#interface Dot11Radio 0 !--- Enter dot11 radio0 interface mode. AP<config-if>#ip access-group TEST in !--- Apply the standard NACL to the radio interface.
```

## Filtres utilisant des listes d'accès étendues

Les listes de contrôle d'accès étendues comparent les adresses source et de destination des paquets IP aux adresses configurées dans la liste de contrôle d'accès pour contrôler le trafic. Les listes de contrôle d'accès étendues fournissent également un moyen de filtrer le trafic en fonction de protocoles de routage spécifiques. Ceci fournit un contrôle plus précis pour l'implémentation des filtres sur un réseau WLAN.

Les listes de contrôle d'accès étendues permettent à un client d'accéder à certaines ressources sur le réseau mais pas à toutes. Par exemple, vous pouvez implémenter un filtre qui autorise le trafic DHCP et Telnet au client tandis qu'il restreint tout autre trafic.

Voici la syntaxe de commande des listes de contrôle d'accès étendues :

**Remarque:** Cette commande est répartie sur quatre lignes pour des raisons d'espace.

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]
```

Dans la version du logiciel Cisco IOS 12.3(7)JA, les listes de contrôle d'accès étendues peuvent utiliser des numéros dans la plage 100 à 199. Les listes de contrôle d'accès étendues peuvent également utiliser des numéros dans la plage de 2000 à 2699. C'est la plage étendue des listes de contrôle d'accès étendues.

**Remarque:** Le mot clé **log** à l'extrémité de chaque entrée de liste ACL indique :

- le numéro et le nom de l'ACL ;
- si le paquet a été autorisé ou refusé ;
- les informations spécifiques au port.

Les listes de contrôle d'accès étendues peuvent également utiliser des noms au lieu des numéros. C'est la syntaxe pour créer des NACL étendues :

```
ip access-list extended name {deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]
```

Cet exemple de configuration utilise des NACL étendues. La condition requise est que la NACL étendue doit permettre l'accès Telnet aux clients. Vous devez restreindre tous les autres protocoles sur le réseau WLAN. En outre, les clients utilisent DHCP afin d'obtenir l'adresse IP.

Vous devez créer une liste de contrôle d'accès étendue qui :

- permet le trafic DHCP et Telnet ;
- refuse tous les autres types de trafic.

Une fois que cette liste de contrôle d'accès étendue est appliquée à l'interface radio, les clients s'associent à l'AP et obtiennent une adresse IP du serveur DHCP. Les clients peuvent également utiliser Telnet. Tous les autres types de trafic sont refusés.

Effectuez ces étapes afin de créer une liste de contrôle d'accès étendue sur l'AP :

1. Connectez-vous à l'AP par la CLI.Utilisez le port de console ou Telnet afin d'accéder à l'ACL par l'interface Ethernet ou l'interface sans fil.
2. Passez en mode de configuration globale sur l'AP :`AP#configure terminal`
3. Exécutez ces commandes afin de créer la liste de contrôle d'accès étendue :`AP<config>#ip access-list extended Allow_DHCP_Telnet !--- Create an extended ACL Allow_DHCP_Telnet. AP<config-extd-nacl>#permit tcp any any eq telnet !--- Allow Telnet traffic. AP<config-extd-nacl>#permit udp any any eq bootpc !--- Allow DHCP traffic. AP<config-extd-nacl>#permit udp any any eq bootps !--- Allow DHCP traffic. AP<config-extd-nacl>#deny ip any any !--- Deny all other traffic types. AP<config-extd-nacl>#exit !--- Return to global configuration mode.`
4. Exécutez ces commandes afin d'appliquer l'ACL à l'interface radio :`AP<config>#interface Dot11Radio 0 AP<config-if>#ip access-group Allow_DHCP_Telnet in !--- Apply the extended ACL Allow_DHCP_Telnet !--- to the radio0 interface.`

## Filtres utilisant des listes de contrôle d'accès basées sur MAC

Vous pouvez utiliser des filtres basés sur l'adresse MAC afin de filtrer des périphériques clients basés sur l'adresse MAC encodée. Quand un client se voit refuser l'accès par un filtre basé sur l'adresse MAC, il ne peut pas s'associer à l'AP. Les filtres d'adresse MAC permettent ou rejettent le transfert des paquets de monodiffusion et de multidiffusion qui sont envoyés depuis ou adressés à des adresses MAC spécifiques.

Voici la syntaxe de commande pour créer une ACL basée sur l'adresse MAC sur l'AP :

**Remarque:** Cette commande a été répartie sur deux lignes pour des raisons d'espace.

**access-list** *access-list-number* **{permit | deny}** *48-bit-hardware-address 48-bit-hardware-address-mask*

Dans la version du logiciel Cisco IOS 12.3(7)JA, les listes de contrôle d'accès d'adresse MAC peuvent utiliser des numéros dans une plage de 700 à 799 comme numéro d'ACL. Elles peuvent également utiliser des numéros dans une plage de 1100 à 1199.

Cet exemple montre comment configurer un filtre basé sur l'adresse MAC par la CLI, afin de filtrer le client avec une adresse MAC **0040.96a5.b5d4** :

1. Connectez-vous à l'AP par la CLI.Utilisez le port de console ou Telnet afin d'accéder à l'ACL par l'interface Ethernet ou l'interface sans fil.
2. Passez en mode de configuration globale sur la CLI de l'AP :`AP#configure terminal`
3. Créez une ACL d'adresse MAC numéro 700.Cette ACL ne permet pas au client 0040.96a5.b5d4 de s'associer à l'AP.
   `access-list 700 deny 0040.96a5.b5d4 0000.0000.0000 !--- This ACL denies all traffic to and from !--- the client with MAC address 0040.96a5.b5d4.`

4. Exécutez cette commande afin d'appliquer cette ACL basée sur l'adresse MAC à l'interface radio :
   **dot11 association mac-list 700** *!--- Apply the MAC-based ACL.*

Après avoir configuré ce filtre sur l'AP, le client avec cette adresse MAC, qui a été précédemment associée à l'AP, est dissocié. La console de l'AP envoie ce message :

```
AccessPoint# *Mar 1 01:42:36.743: %DOT11-6-DISASSOC: Interface
 Dot11Radio0, Deauthenticating Station 0040.96a5.b5d4
```

### Filtres utilisant des listes de contrôle d'accès basées sur l'heure

Les listes de contrôle d'accès basées sur l'heure peuvent être activées ou désactivées pour une période de temps spécifique. Cette fonctionnalité offre la robustesse et la souplesse permettant de définir des stratégies de contrôle d'accès qui autorisent ou refusent certains types de trafic.

Cet exemple montre comment configurer une ACL basée sur le temps par la CLI, où la connexion Telnet est autorisée depuis le réseau vers l'extérieur en semaine et pendant les heures ouvrables :

**Remarque:** Une ACL basée sur le temps peut être définie sur le port Fast Ethernet ou sur le port Radio de l'AP Aironet, en fonction des besoins. Elle n'est jamais appliquée sur le Bridge Group Virtual Interface (BVI).

1. Connectez-vous à l'AP par la CLI.Utilisez le port de console ou Telnet afin d'accéder à l'ACL par l'interface Ethernet ou l'interface sans fil.
2. Passez en mode de configuration globale sur la CLI de l'AP :`AP#`**`configure terminal`**
3. Créez une plage horaire. Pour cela, exécutez cette commande en mode de configuration globale :`AP<config>#`**`time-range Test`** *!--- Create a time-range with name Test.* `AP(config-time-range)#` **`periodic weekdays 7:00 to 19:00`** *!--- Allows access to users during weekdays from 7:00 to 19:00 hrs.*
4. Créez une ACL 101 :`AP<config>#` **`ip access-list extended 101`** `AP<config-ext-nacl>#`**`permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range Test`** *!--- This ACL permits Telnet traffic to and from !--- the network for the specified time-range Test.* Cette ACL autorise une session Telnet à l'AP en semaine.
5. Exécutez cette commande afin d'appliquer cette ACL basée sur le temps à l'interface Ethernet :
   **interface Ethernet0/0 ip address 10.1.1.1 255.255.255.0 ip access-group 101 in** *!--- Apply the time-based ACL.*

## Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannez

Utilisez cette section pour dépanner votre configuration.

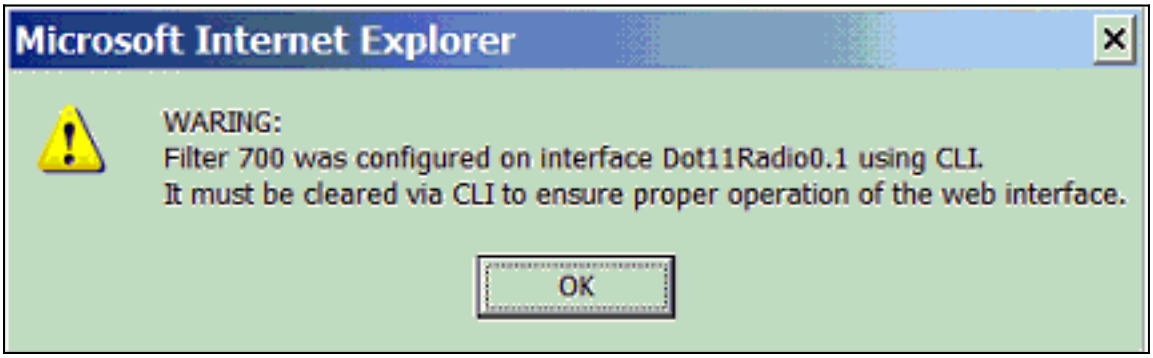
Effectuez ces étapes afin de supprimer une ACL d'une interface :

1. Passez en mode de configuration de l'interface.
2. Entrez **no** devant la commande **ip access-group**, comme le montre cet exemple :

```
interface interface no ip access-group {access-list-name | access-list-number} {in | out}
```

Vous pouvez également utiliser la commande **show access-list name | number** afin de dépanner votre configuration. La commande **show ip access-list** fournit un nombre de paquets qui indique l'entrée de la liste de contrôle d'accès consultée.

Évitez d'utiliser à la fois la CLI et les interfaces de navigateur Web pour configurer le périphérique sans fil. Si vous configurez le périphérique sans fil avec la CLI, l'interface de navigateur Web peut afficher une traduction inexacte de la configuration. Cependant, cette inexactitude ne signifie pas nécessairement que le périphérique sans fil est mal configuré. Par exemple, si vous configurez les ACL avec la CLI, l'interface de navigateur Web peut afficher ce message :




Si vous voyez ce message, utilisez la CLI afin de supprimer les ACL et utilisez l'interface de navigateur Web pour les reconfigurer.

## Informations connexes

- Configuration des filtres
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems