Exemple de configuration de listes de contrôle d'accès sur un contrôleur de réseau local sans fil

Contenu

Introduction

Ce document explique comment configurer le Listes de contrôle d'accès (ACL) sur les contrôleurs LAN Sans fil (WLCs) afin de filtrer le trafic qui écrit et part d'un WLAN.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La connaissance de la façon configurer le WLC et le point d'accès léger (LAP) pour le fonctionnement de base
- Connaissance de base du protocole de point d'accès léger (LWAPP) et des méthodes de sécurité sans fil

Composants utilisés

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

- Gamme Cisco 2000 WLC qui exécute les micrologiciels 4.0

- RECOUVREMENT de gamme Cisco 1000
- Adaptateur client sans fil de Cisco 802.11a/b/g qui exécute le micrologiciel 2.6
- Version 2.6 de Cisco Aironet Desktop Utility (ADU)

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.

ACLs sur WLCs

ACLs sur le WLC sont censés pour limiter ou permettre des clients sans fil aux services sur son WLAN.

Avant version 4.0 de micrologiciels WLC, ACLs sont sautés sur l'interface de gestion, ainsi vous ne pouvez pas affecter le trafic destiné au WLC autres qu'empêcher les clients Sans fil de gérer le contrôleur avec l'option de **Management via Wireless**. Par conséquent, ACLs peut seulement être appliqué aux interfaces dynamiques. Dans la version 4.0 de micrologiciels WLC, il y a CPU ACLs qui peut filtrer le trafic destiné pour l'interface de gestion. Un exemple de la façon configurer CPU ACLs est fourni plus tard dans ce document.

Vous pouvez définir jusqu'à 64 ACLs, chacun avec jusqu'à 64 règles (ou filtres). Chaque règle a les paramètres qui affectent son action. Quand un paquet apparie tous les paramètres pour une règle, l'action réglée pour cette règle est appliquée au paquet. Vous pouvez configurer ACLs par le GUI ou le CLI.

Ce sont certaines des règles que vous devez comprendre avant que vous configuriez un ACL sur le WLC :

- Si la source *et la* destination en sont, la direction dans laquelle cet ACL est appliqué en peut être.
- Si la source *ou la* destination n'en sont pas, alors la direction du filtre doit être spécifiée, et une déclaration inverse dans le sens inverse doit être créée.
- La notion Du WLC d'arrivée contre sortant est nonintuitive. Il est de la perspective du WLC faisant face vers le client sans fil, plutôt que de la perspective du client. Ainsi, la direction d'arrivée signifie qu'un paquet qui entre dans le WLC du client sans fil et de la direction sortante signifie un paquet ce des sorties du WLC vers le client sans fil.
- Il y a un implicite refusent à la fin de l'ACL.

Considérations en configurant ACLs dans WLCs

ALCs dans le travail de WLCs différemment que dans des Routeurs. Ce sont quelques choses à se souvenir quand vous configurez ACLs dans WLCs :

- L'erreur la plus commune est de sélectionner l'IP quand vous avez l'intention de refuser ou

permettre des paquets IP. Puisque vous sélectionnez ce qui est à l'intérieur du paquet IP, vous finissez par refuser ou permettre des paquets d'IP-in-IP.
- Le contrôleur ACLs ne peut pas bloquer 1.1.1.1 (adresse IP virtuelle), et par conséquent des paquets DHCP pour des clients sans fil.
- Le contrôleur ACLs ne peut pas bloquer le trafic de multidiffusion reçu des réseaux câblés qui est destiné aux clients sans fil. Le contrôleur ACLs sont traités pour le trafic de multidiffusion initié des clients sans fil, destinés aux réseaux câblés ou à d'autres clients sans fil sur le même contrôleur.
- Àla différence d'un routeur, les contrôles d'ACL trafiquent des deux directions une fois appliqués à une interface, mais elle n'exécute pas l'avec état firewalling. Si vous oubliez d'ouvrir un trou dans l'ACL pour le trafic de renvoi, ceci pose un problème.
- Paquets IP de bloc d'ACLs de contrôleur seulement. Vous ne pouvez pas bloquer la couche 2 ACLs ou poser 3 paquets qui ne sont pas IP.
- Le contrôleur ACLs n'utilisent pas les masques inverses comme les Routeurs. Ici, 255 signifie la correspondance cet octet de l'adresse IP exactement.
- ACLs sur le contrôleur sont faits dans la représentation d'expédition de logiciel et d'incidence.

Note: Si vous vous appliquez un ACL à une interface ou à un WLAN, le débit Sans fil est dégradé et peut mener à la perte potentielle de paquets. Afin d'améliorer le débit, retirer l'ACL de l'interface ou du WLAN et déplacer l'ACL à un périphérique de câble voisin.

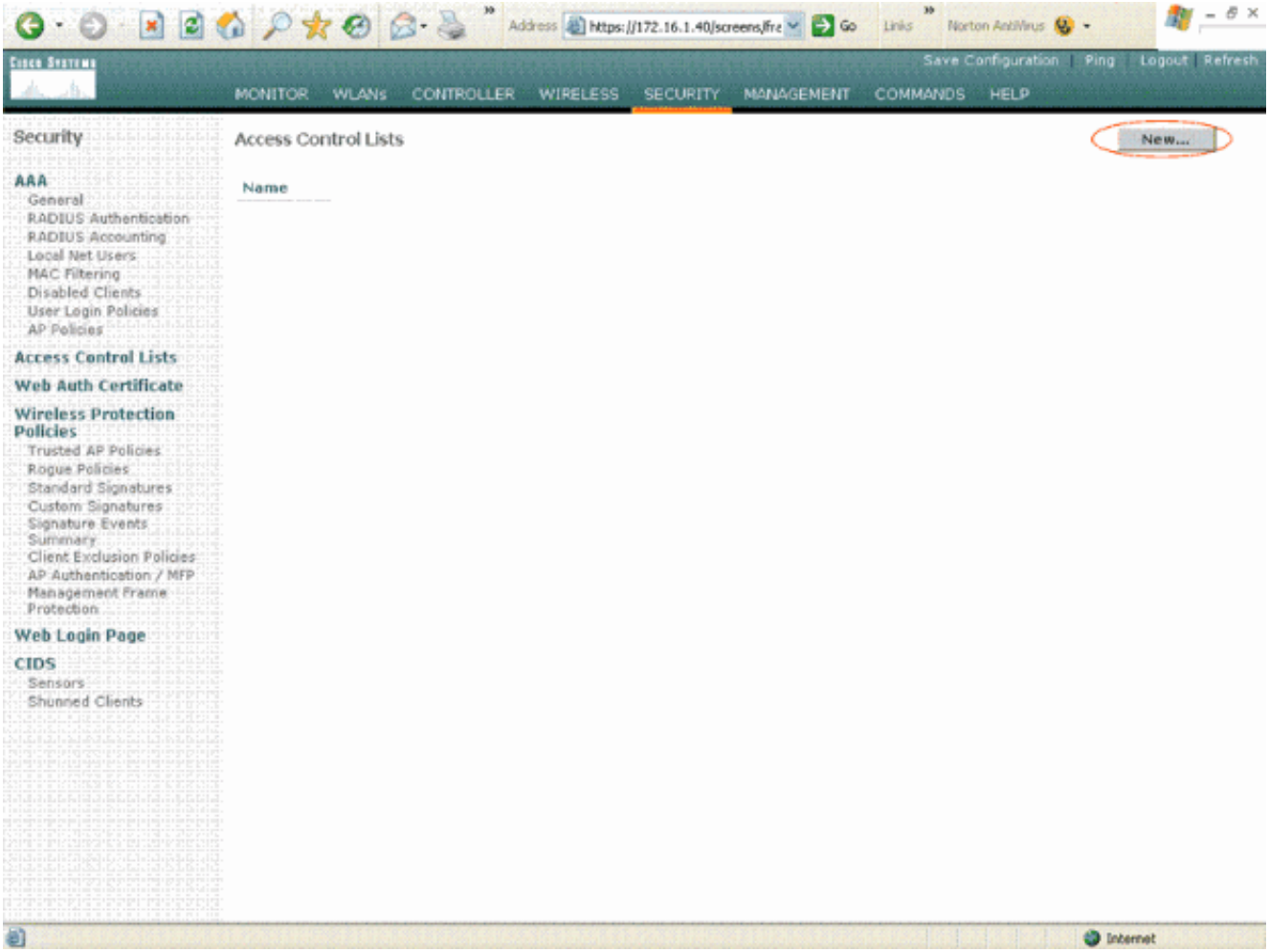
Configurez l'ACL sur WLCs

Cette section décrit comment configurer un ACL sur le WLC. L'objectif est de configurer un ACL qui permet à des clients d'invité pour accéder à ces services :

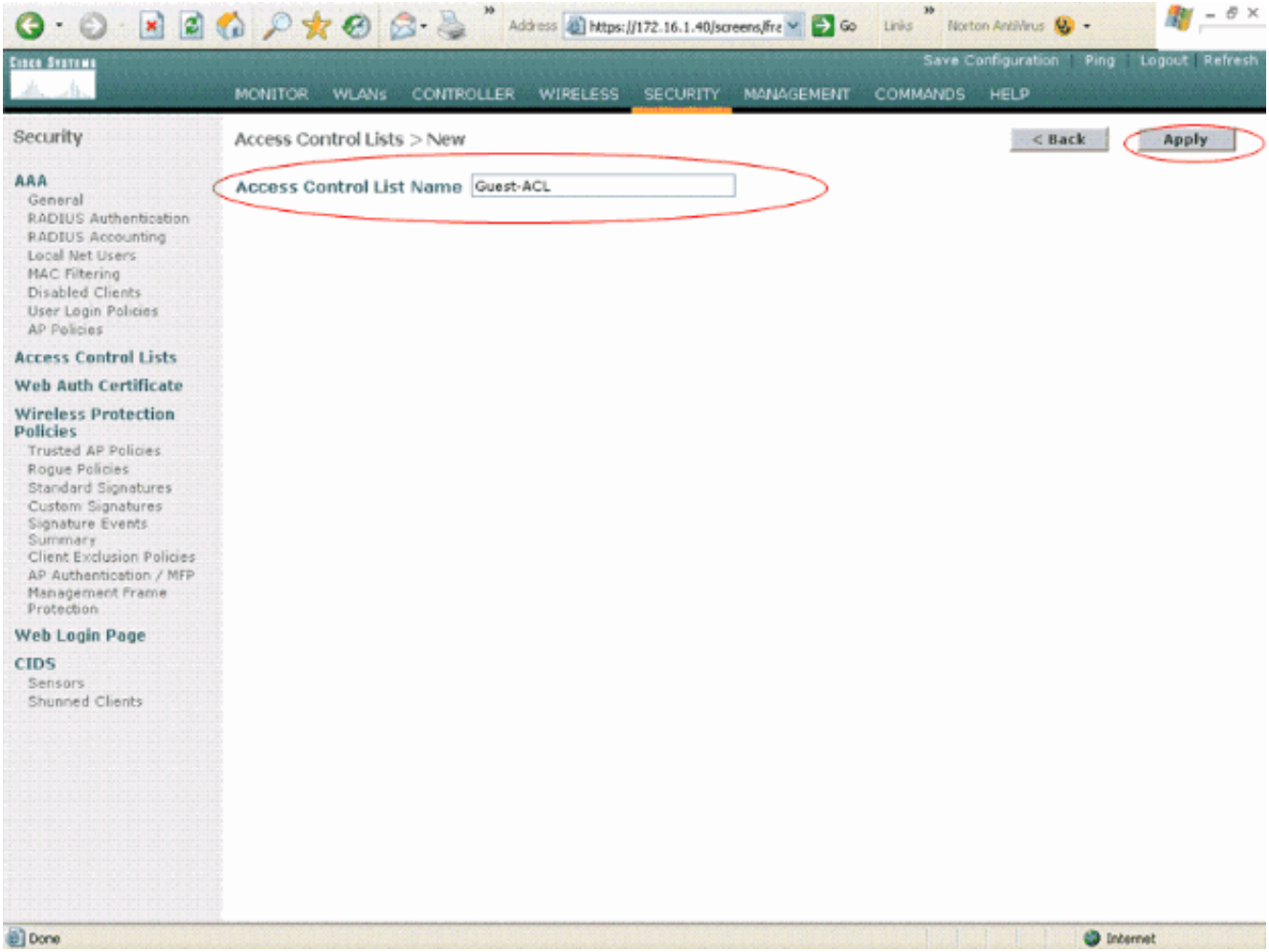
- Protocole DHCP (DHCP) entre les clients sans fil et le serveur DHCP
- Protocole ICMP (Internet Control Message Protocol) entre tous les périphériques dans le réseau
- Système de noms de domaine (DNS) entre les clients sans fil et le serveur DNS
- Telnet à un sous-réseau spécifique

Tous autres services doivent être bloqués pour les clients sans fil. Terminez-vous ces étapes afin de créer l'ACL utilisant le GUI WLC :

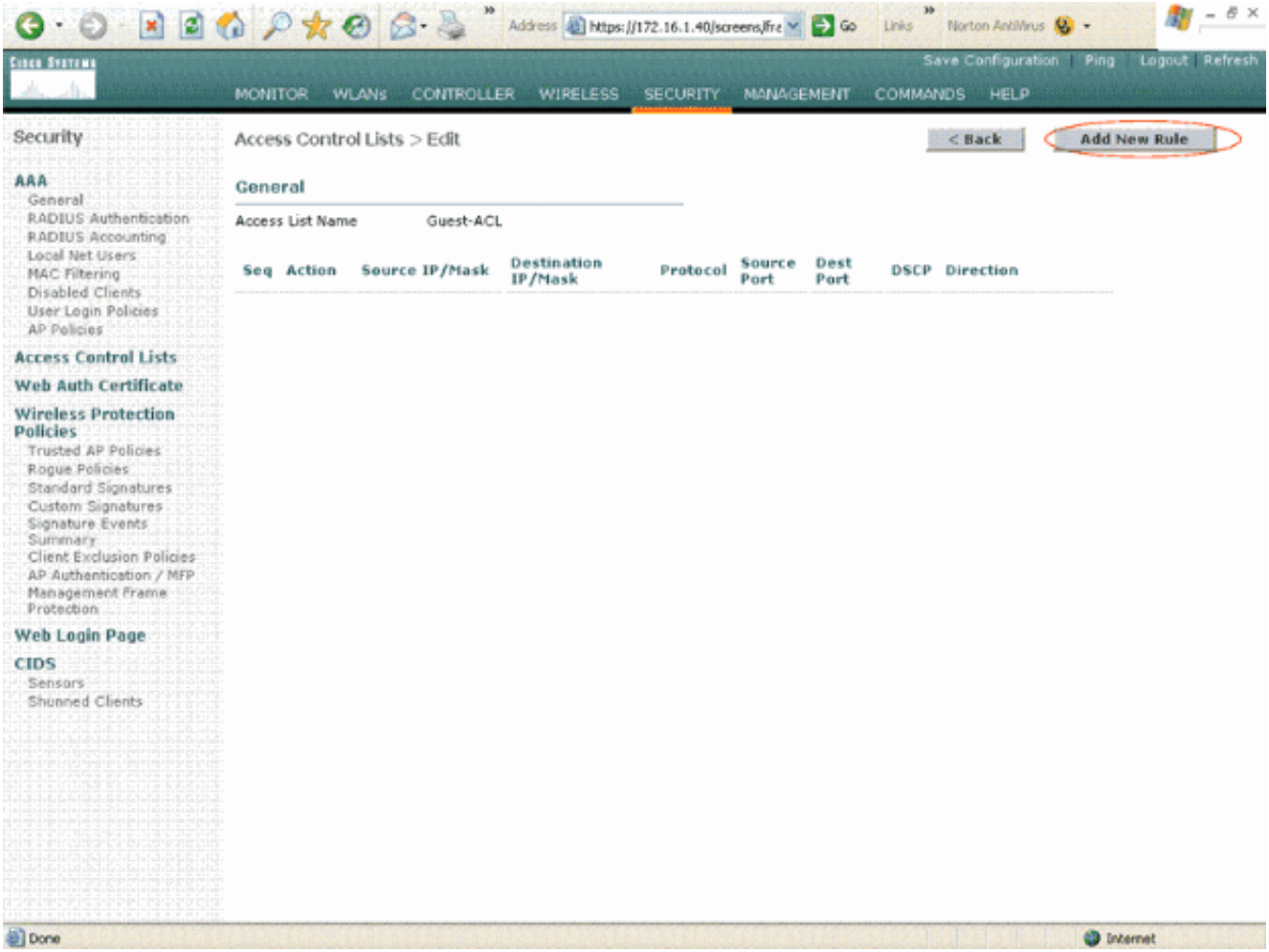
1. Allez au GUI WLC et choisissez la **Sécurité > les listes de contrôle d'accès**.La page de listes de contrôle d'accès paraît. Cette page répertorie l'ACLs qui sont configurés sur le WLC. Il te permet également d'éditer ou retirer ACLs l'un des. Afin de créer un nouvel ACL, cliquez sur New.



2. Écrivez le nom de l'ACL et cliquez sur Apply.Vous pouvez écrire jusqu'à 32 caractères alphanumériques. Dans cet exemple, le nom de l'ACL est Invité-**ACL**. Une fois que l'ACL est créé, cliquez sur Edit afin de créer des règles pour l'ACL.



3. Quand les listes de contrôle d'accès > éditent la page paraît, clique sur Add la **nouvelle règle**.Les listes de contrôle d'accès > ordonne > nouvelle page apparaît.



4. Configurez les règles qui permettent à un utilisateur d'invité ces services :DHCP entre les clients sans fil et le serveur DHCPICMP entre tous les périphériques dans le réseauDN entre les clients sans fil et le serveur DNSTelnet à un sous-réseau spécifique

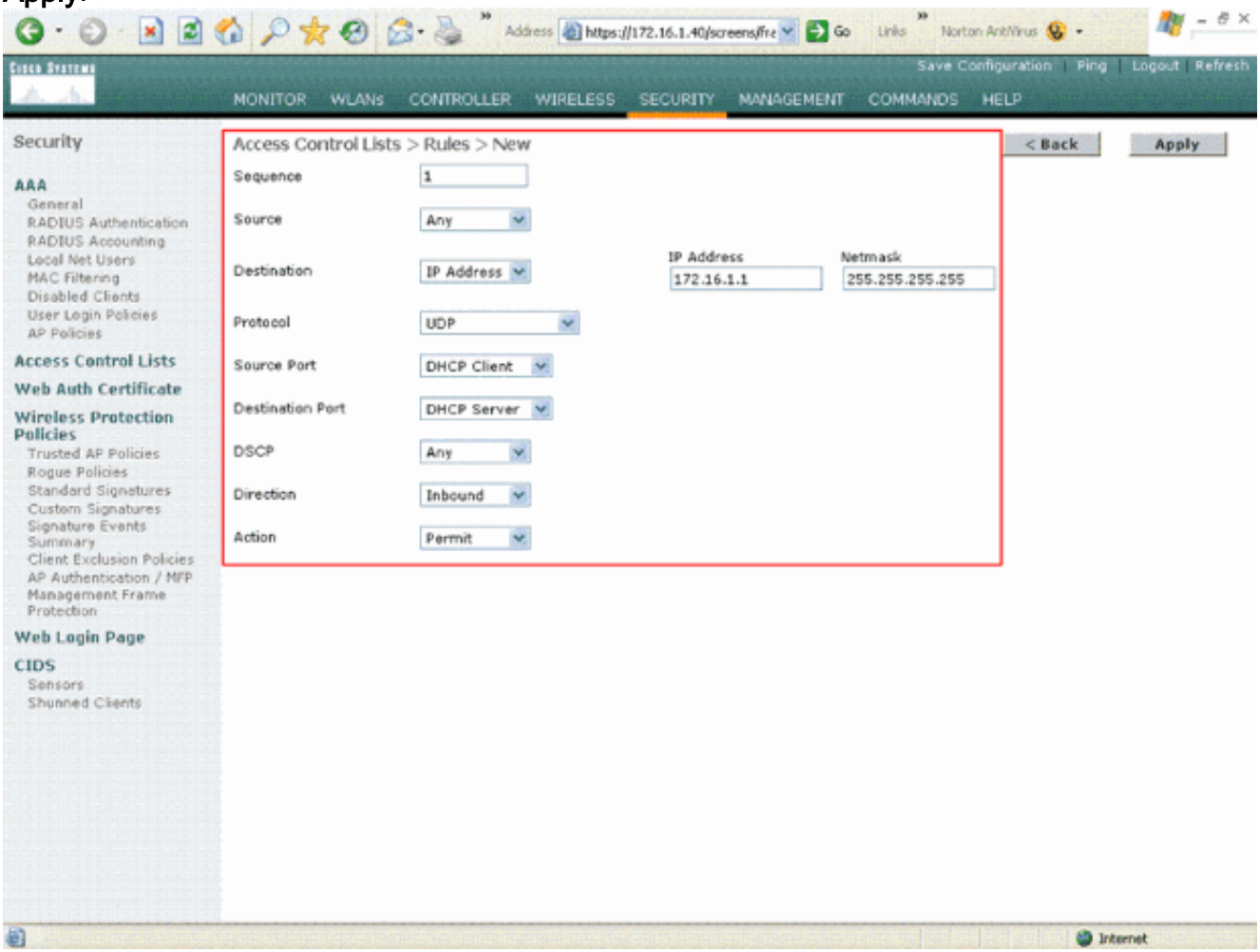
Configurez les règles qui permettent des services d'utilisateur d'invité

Cette section affiche un exemple pour que la façon configure les règles pour ces services :

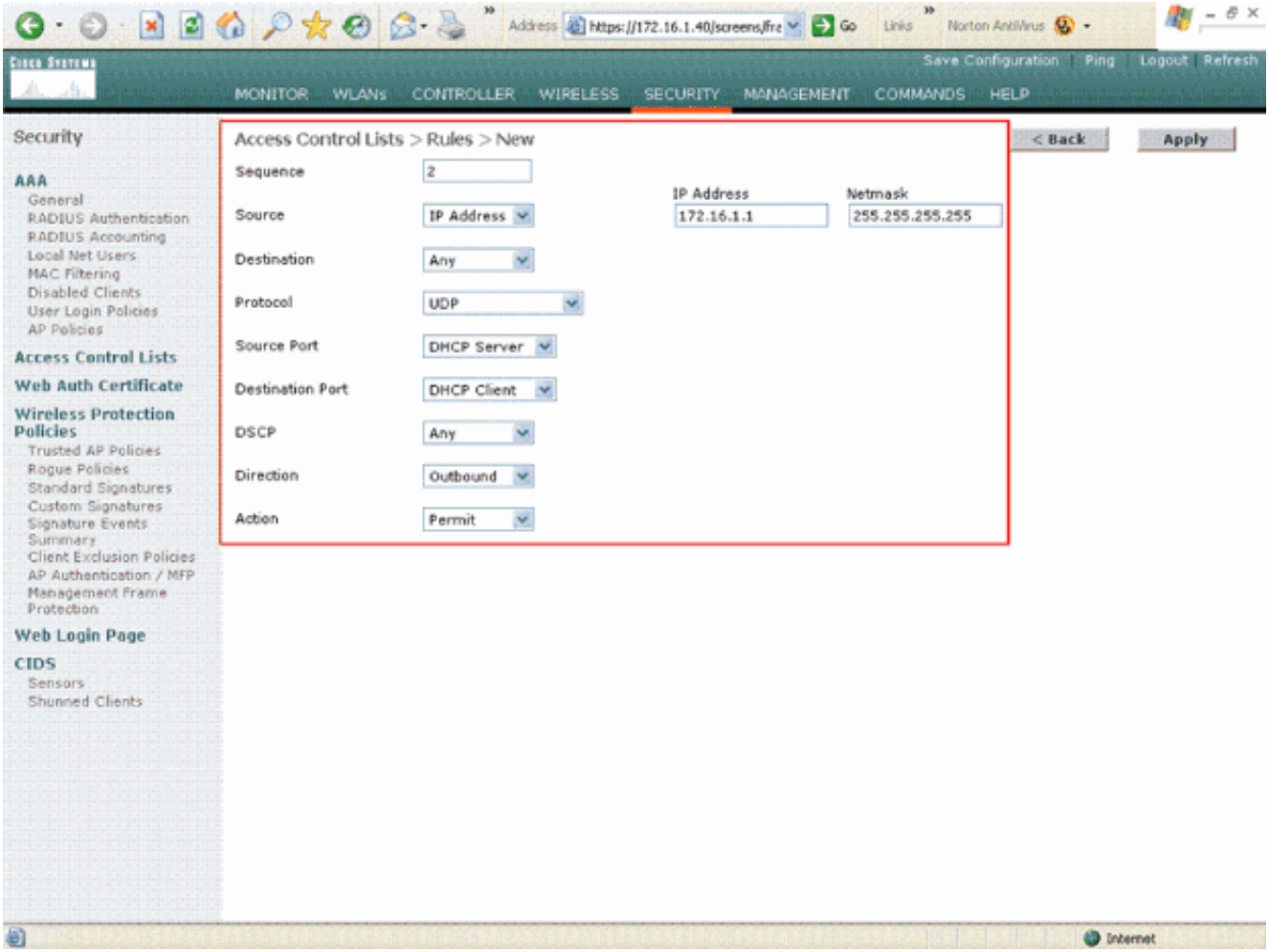
- DHCP entre les clients sans fil et le serveur DHCP
- ICMP entre tous les périphériques dans le réseau
- DN entre les clients sans fil et le serveur DNS
- Telnet à un sous-réseau spécifique

1. Afin de définir la règle pour le service DHCP, sélectionnez les plages IP de source et de destination.Cet exemple en utilise pour la source qui signifie qu'à n'importe quel client sans fil est permis l'accès au serveur DHCP. Dans cet exemple, le serveur 172.16.1.1 agit en tant que DHCP et serveur DNS. Ainsi, l'adresse IP de destination est 172.16.1.1/255.255.255.255 (avec un masque d'hôte).Puisque le DHCP est un protocole basé par UDP, **UDP** choisi du champ de déroulant de Protocol. Si vous choisissiez le TCP ou l'UDP dans l'étape précédente, deux paramètres supplémentaires apparaissent : Port et destination port de source. Spécifiez les détails de source et de destination port. Pour cette règle, le port de source est **DHCP Client** et la destination port est **serveur DHCP**.Choisissez la direction dans laquelle l'ACL doit être appliqué. Puisque cette règle est du client au serveur, des utilisations de cet exemple **d'arrivée**. De la liste déroulante d'action, choisissez l'**autorisation** de faire permettre cet ACL des paquets DHCP du client sans fil au serveur

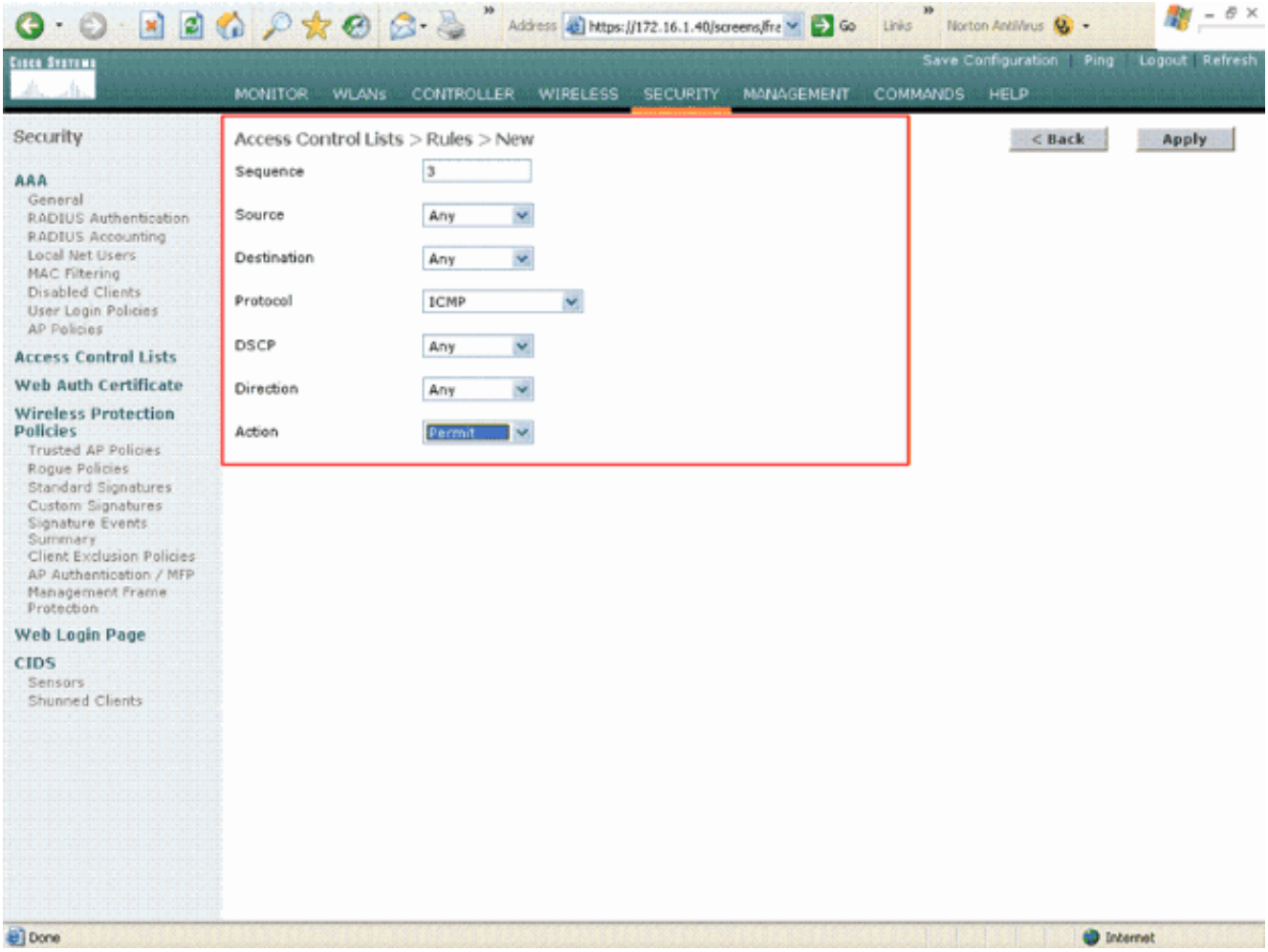
DHCP. La valeur par défaut est refusent. Cliquez sur **Apply**.



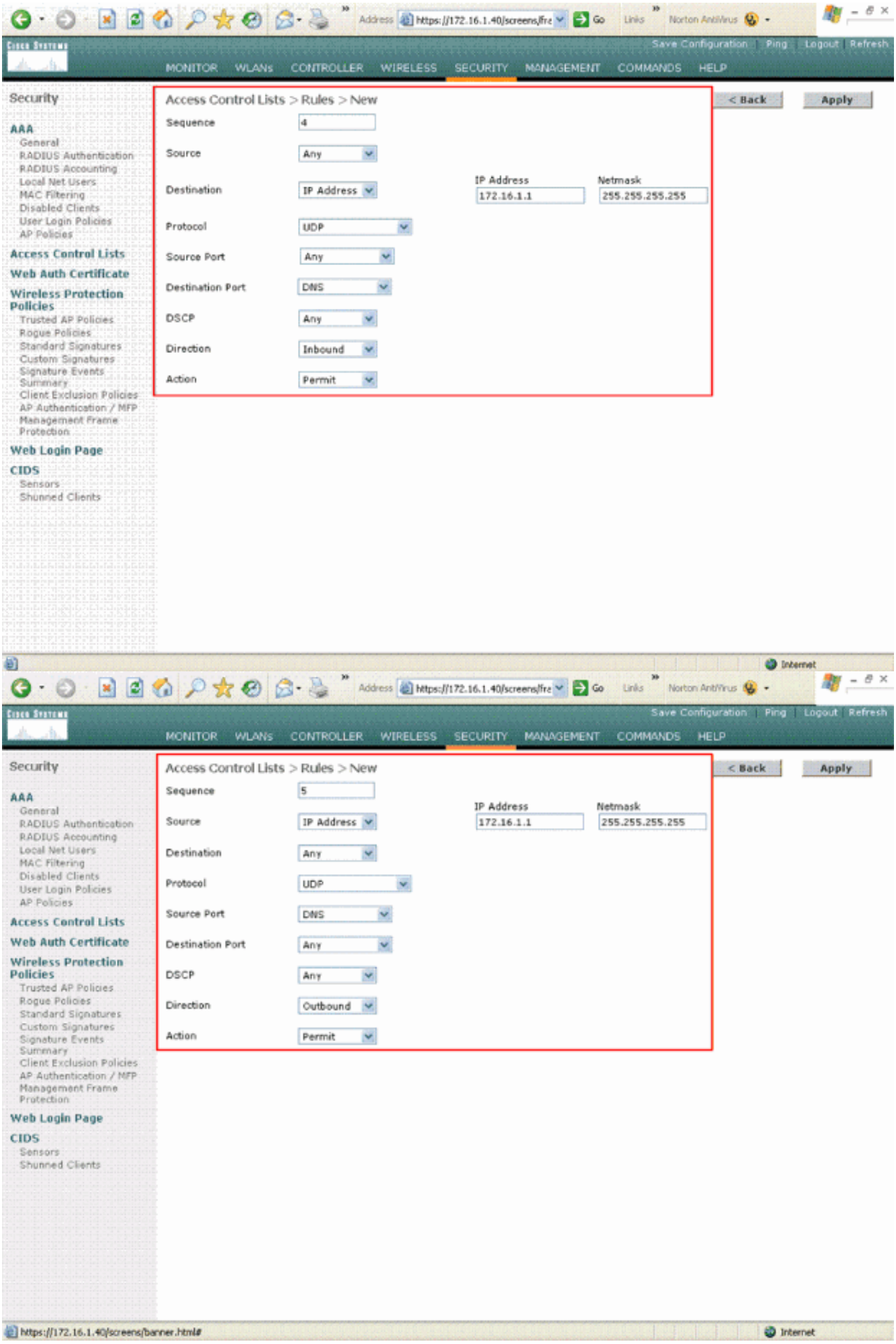
Si la source ou la destination n'en sont pas, alors une déclaration inverse dans le sens inverse doit être créée. Voici un exemple.



2. Afin de définir une règle qui permet des paquets d'ICMP entre tous les périphériques, en sélectionnez pour la source et les champs de destination. C'est la valeur par défaut.Choisissez l'**ICMP du** champ de déroulant de Protocol. Puisque cet exemple en utilise pour la source et les champs de destination, vous ne devez pas spécifier la direction. Il en peut être laissé à sa valeur par défaut de. En outre, la déclaration inverse dans le sens inverse n'est pas exigée.Du menu déroulant d'action, choisissez l'**autorisation** afin de faire permettre cet ACL des paquets DHCP du serveur DHCP au client sans fil. Cliquez sur **Apply**.

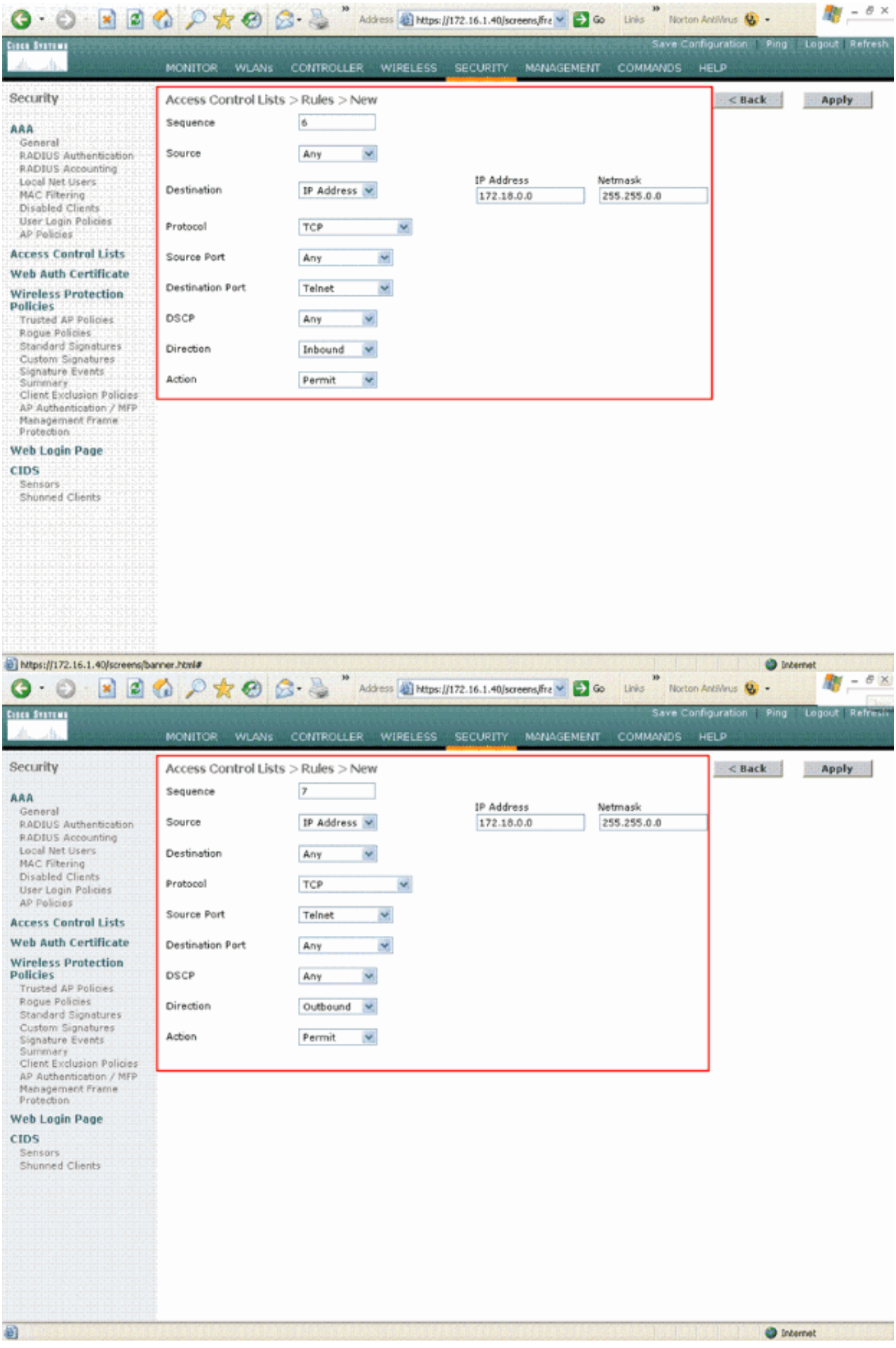


3. De même, créez les règles qui permettent l'accès de serveur DNS à tous les clients sans fil et l'accès de serveur telnet pour le client sans fil à un sous-réseau spécifique. Voici les exemples.

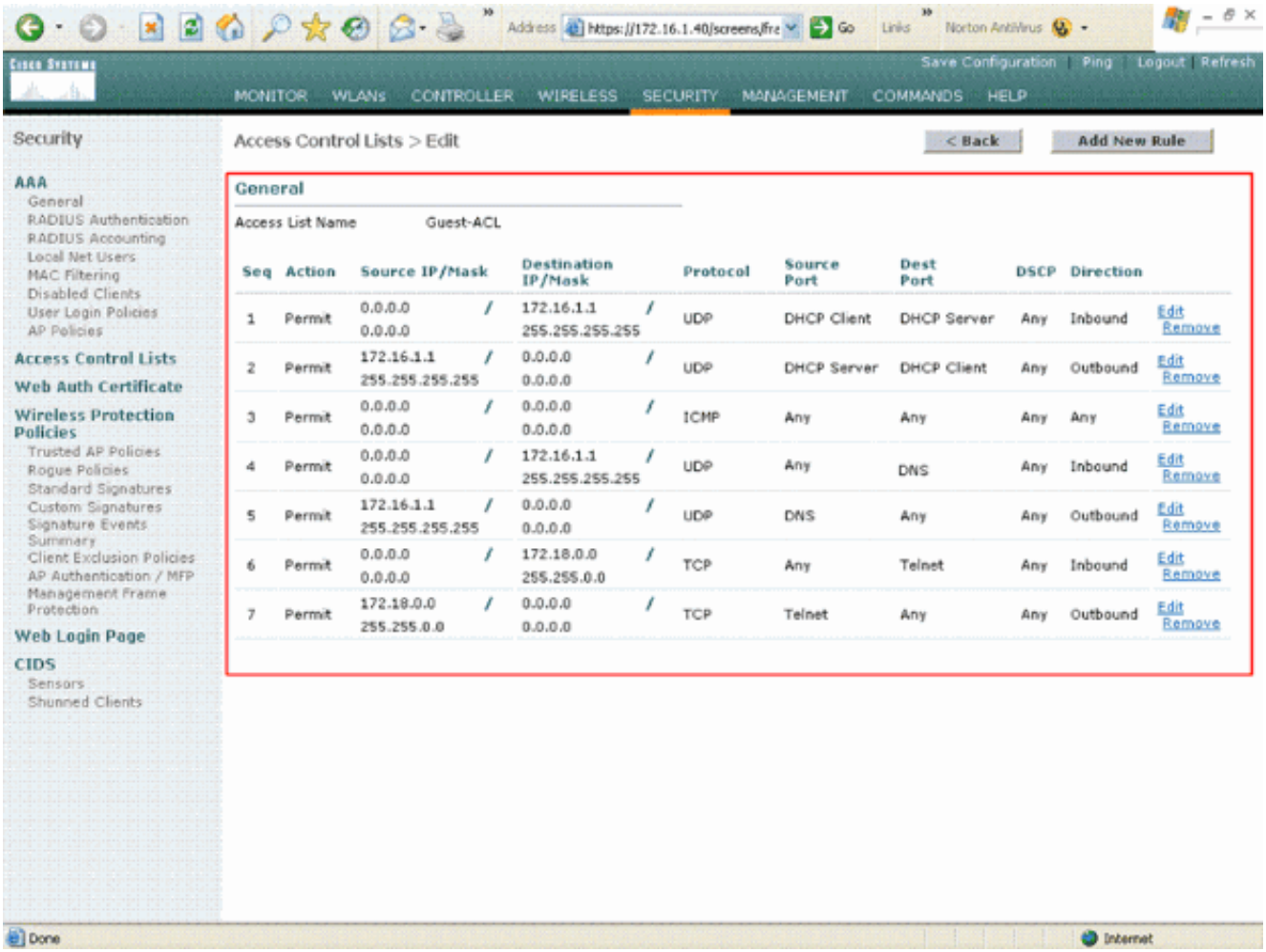


Définissez cette règle afin de permettre l'accès pour le client sans fil au service

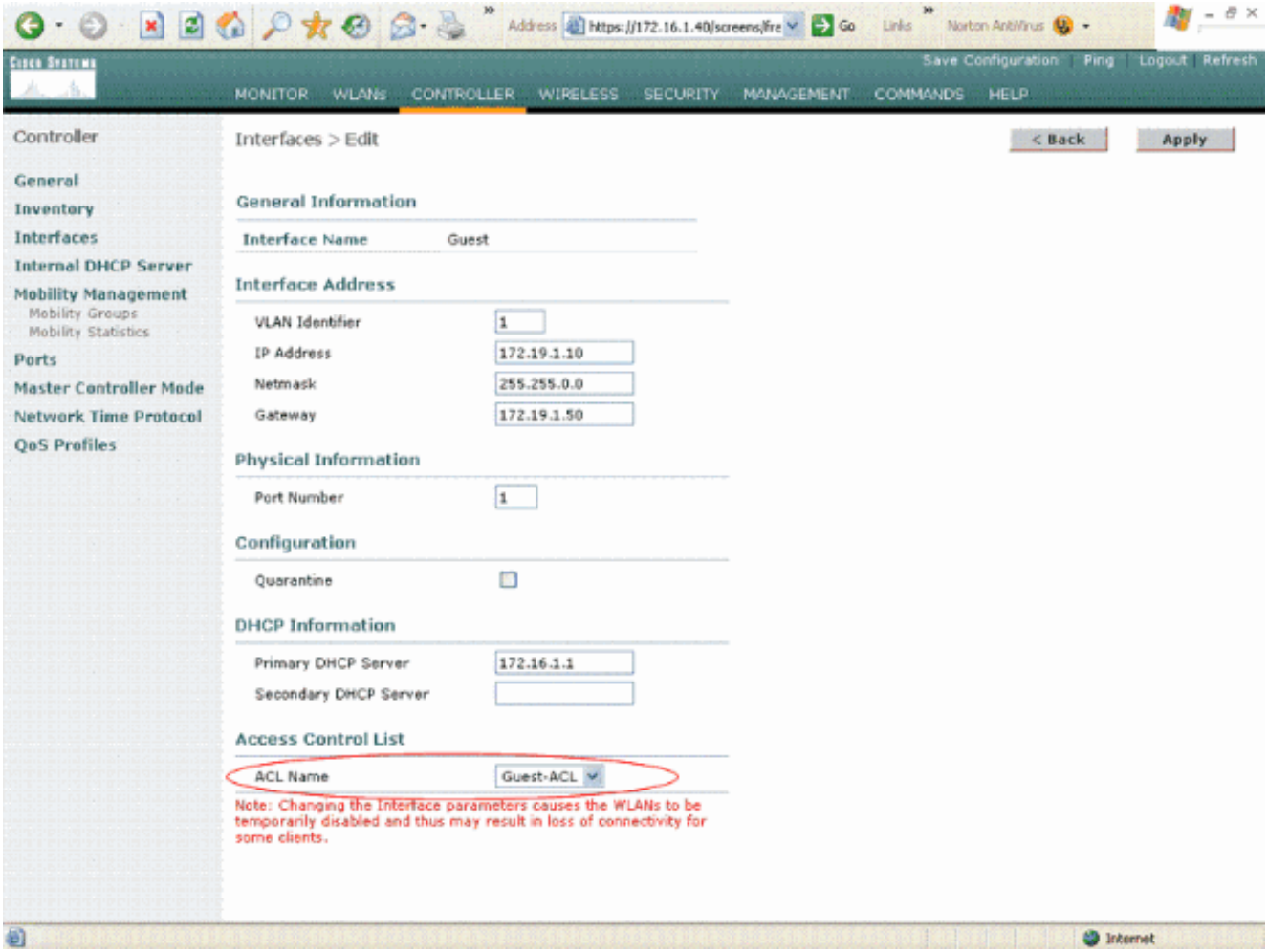
Telnet.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Signature Events Summary
Client Exclusion Policies
AP Authentication / MFP
Management Frame Protection
Web Login Page
CIDS
Sensors
Shunned Clients
Access Control Lists > Rules > New
< Back
Apply
Sequence
6
Source
Any
Destination
IP Address
IP Address
172.18.0.0
Netmask
255.255.0.0
Protocol
TCP
Source Port
Any
Destination Port
Telnet
DSCP
Any
Direction
Inbound
Action
Permit
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Access Control Lists
Web Auth Certificate
Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Signature Events Summary
Client Exclusion Policies
AP Authentication / MFP
Management Frame Protection
Web Login Page
CIDS
Sensors
Shunned Clients
Access Control Lists > Rules > New
< Back
Apply
Sequence
7
Source
IP Address
IP Address
172.18.0.0
Netmask
255.255.0.0
Destination
Any
Protocol
TCP
Source Port
Telnet
Destination Port
Any
DSCP
Any
Direction
Outbound
Action
Permit

L'ACL > éditent la page répertorie toutes les règles qui sont définies pour l'ACL.



4. Une fois que l'ACL est créé, il doit être appliqué à une interface dynamique. Afin d'appliquer l'ACL, choisissez le **Controller > Interfaces** et éditez l'interface à laquelle vous voulez s'appliquer l'ACL.
5. Dans la page d'**Interfaces > Edit** pour l'interface dynamique, choisissez l'ACL approprié du menu déroulant de listes de contrôle d'accès. Voici un exemple.



Une fois que ceci est fait, l'ACL permet et refuse le trafic (basé sur les règles configurées) sur le WLAN qui utilise cette interface dynamique. L'Interface-ACL peut seulement être appliqué H-pour récolter des aps en mode connecté mais pas en mode autonome.

Note: Référez-vous utilisant le CLI pour configurer des listes de contrôle d'accès pour les informations sur la façon dont créer un ACL avec le CLI sur le WLC.

Note: Ce document suppose que des WLAN et les interfaces dynamiques sont configurés. Référez-vous aux VLAN sur l'exemple Sans fil de configuration de contrôleurs LAN pour les informations sur la façon dont créer des interfaces dynamiques sur WLCs.

Configurez CPU ACLs

Précédemment, ACLs sur WLCs n'a pas eu une option de filtrer le trafic du trafic de données LWAPP/CAPWAP, de contrôle LWAPP/CAPWAP, et le trafic de mobilité destiné aux interfaces de Gestion et de gestionnaire AP. Afin d'aborder ces question et filtre LWAPP et mobilité trafiquez, CPU ACLs ont été introduits avec la version de microprogramme 4.0 WLC.

La configuration de CPU ACLs implique deux étapes :

1. Configurez les règles pour l'ACL CPU.
2. Appliquez l'ACL CPU sur le WLC.

Les règles pour l'ACL CPU devraient être configurées d'une manière semblable à l'autre ACLs. Référez-vous à la section CPU ACLs de sécuriser les contrôleurs LAN Sans fil (WLCs) pour plus d'informations sur CPU ACLs.

Vérifiez

Cisco recommande que vous testiez vos configurations d'ACL avec un client sans fil afin de s'assurer que vous les avez configurées correctement. S'ils n'opèrent pas correctement, vérifiez l'ACLs sur la page Web d'ACL et le vérifiez que vos modifications d'ACL ont été appliquées à l'interface du contrôleur.

Vous pouvez également employer ces **commandes show** afin de vérifier votre configuration :

- **résumé de show acl** — Afin d'afficher l'ACLs qui sont configurés sur le contrôleur, utilisez la commande de **résumé de show acl**.Voici un exemple :

```
(Cisco Controller) >show acl summary

ACL Name                         Applied
-------------------------------- -------
Guest-ACL                        Yes
```

- **show acl *ACL_Name* détaillé** — Affiche les informations détaillées sur l'ACLs configuré.Voici un exemple :

```
(Cisco Controller) >show acl detailed Guest-ACL

                  Source                        Destination               Source Port
Dest Port
I  Dir       IP Address/Netmask             IP Address/Netmask        Prot    Range
Range    DSCP Action
-- --- ------------------------------ ------------------------------ ---- ---------- ----
------- ---- ------
 1  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17    68-68
67-67     Any Permit
 2 Out      172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    67-67
68-68     Any Permit
 3 Any        0.0.0.0/0.0.0.0                 0.0.0.0/0.0.0.0            1     0-65535
0-65535  Any Permit
 4  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17     0-65535
53-53     Any Permit
 5 Out      172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    53-53
0-65535  Any Permit
 6  In         0.0.0.0/0.0.0.0             172.18.0.0/255.255.0.0             60-65535
23-23     Any Permit
 7 Out      172.18.0.0/255.255.0.0             0.0.0.0/0.0.0.0            6    23-23
0-65535  Any Permit
```

- **show acl cpu** — Afin d'afficher l'ACLs configuré sur la CPU, utilisez la commande de **show acl cpu**.Voici un exemple :

```
(Cisco Controller) >show acl detailed Guest-ACL

                  Source                        Destination               Source Port
Dest Port
I  Dir       IP Address/Netmask             IP Address/Netmask        Prot    Range
Range    DSCP Action
-- --- ------------------------------ ------------------------------ ---- ---------- ----
------- ---- ------
 1  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17    68-68
67-67     Any Permit
 2 Out      172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    67-67
68-68     Any Permit
 3 Any        0.0.0.0/0.0.0.0                 0.0.0.0/0.0.0.0            1     0-65535
0-65535  Any Permit
 4  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17     0-65535
53-53     Any Permit
```

```
 5 Out      172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    53-53
0-65535  Any Permit
 6  In         0.0.0.0/0.0.0.0              172.18.0.0/255.255.0.0             60-65535
23-23     Any Permit
 7 Out      172.18.0.0/255.255.0.0             0.0.0.0/0.0.0.0            6    23-23
0-65535  Any Permit
```

Dépannez

La version de logiciel de logiciel contrôleur 4.2.61.0 ou plus tard te permet de configurer des compteurs d'ACL. Les compteurs d'ACL peuvent aider à déterminer quel ACLs ont été appliqués aux paquets transmis par le contrôleur. Cette caractéristique est utile quand vous dépannez votre système.

Les compteurs d'ACL sont disponibles sur ces contrôleurs :

- Gamme 4400
- Cisco WiSM
- Commutateur de contrôleur sans fil LAN intégré du Catalyst 3750G

Afin d'activer cette caractéristique, terminez-vous ces étapes :

1. Choisissez la **Sécurité > les listes de contrôle d'accès > les listes de contrôle d'accès** afin d'ouvrir la page de listes de contrôle d'accès.Cette page répertorie tout les ACLs qui ont été configurés pour ce contrôleur.
2. Afin de voir si les paquets frappent ACLs l'un des configuré sur votre contrôleur, cochez la case de **compteurs d'enable** et cliquez sur Apply. Autrement, laissez la case décochée. C'est la valeur par défaut.
3. Si vous voulez effacer les compteurs pour un ACL, planent votre curseur au-dessus de la flèche déroulante bleue pour cet ACL et choisissent les **compteurs clairs**.

Informations connexes

- Configurant et appliquant des listes de contrôle d'accès
- Exemple de configuration de réseaux VLAN sur des contrôleurs de réseau local sans fil
- Enregistrement d'un point d'accès léger (LAP) sur un contrôleur LAN sans fil (WLC)
- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0
- Support technique sans fil/mobilité
- Support et documentation techniques - Cisco Systems