Exemple de configuration des ACL sur un contrôleur LAN sans fil

Table des matières

Introduction

Ce document décrit comment configurer les listes de contrôle d'accès (ACL) sur les contrôleurs de réseau local sans fil (WLAN) pour filtrer le trafic à travers le WLAN.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment 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 :

- Contrôleur de réseau sans fil de la gamme Cisco 2000 qui exécute le micrologiciel 4.0
- LAP de la gamme Cisco 1000
- Adaptateur client sans fil Cisco 802.11a/b/g qui exécute le microprogramme 2.6
- Utilitaire de bureau Cisco Aironet (ADU) version 2.6

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.

Conventions

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

ACL sur les WLC

Les listes de contrôle d'accès sur le WLC sont destinées à restreindre ou autoriser les clients sans fil à accéder aux services sur son WLAN.

Avant la version 4.0 du microprogramme du WLC, les ACL sont contournées sur l'interface de gestion, de sorte que vous ne pouvez pas affecter le trafic destiné au WLC, vous pouvez seulement empêcher les clients sans fil de la gestion du contrôleur avec l'option **Management Via Wireless**. Par conséquent, les listes de contrôle d'accès peuvent uniquement être appliquées aux interfaces dynamiques. Dans la version 4.0 du microprogramme du WLC, il y a des ACL de CPU qui peuvent filtrer le trafic destiné à l'interface de gestion. Consultez la section Configurer les ACL du processeur pour plus d'informations.

Vous pouvez définir jusqu'à 64 listes de contrôle d'accès, chacune avec jusqu'à 64 règles (ou filtres). Chaque règle possède des paramètres qui affectent son action. Lorsqu'un paquet correspond à tous les paramètres d'une règle, l'action définie pour cette règle est appliquée au paquet. Vous pouvez configurer les listes de contrôle d'accès via l'interface utilisateur graphique ou l'interface de ligne de commande.

Voici quelques règles que vous devez comprendre avant de configurer une liste de contrôle d'accès sur le WLC :

- Si la source et la destination sont **quelconques**, la direction dans laquelle cette liste de contrôle d'accès est appliquée peut être **quelconque** .
- Si l'une ou l'autre des destinations source **n'est pas** définie, la direction du filtre doit être spécifiée et une instruction inverse dans la direction opposée doit être créée.
- La notion WLC de trafic entrant par rapport au trafic sortant n'est pas intuitive. C'est du point de vue du WLC orienté vers le client sans fil, plutôt que du point de vue du client. Ainsi, la direction entrante signifie un paquet qui arrive dans le WLC à partir du client sans fil et la direction sortante signifie un paquet qui sort du WLC vers le client sans fil.
- Il y a un refus implicite à la fin de la liste de contrôle d'accès.

Considérations lorsque des ACL sont configurées dans des WLC

Les ALC des WLC fonctionnent différemment que dans les routeurs. Voici quelques points à retenir lorsque vous configurez des listes de contrôle d'accès dans des WLC :

- L'erreur la plus courante est de sélectionner IP lorsque vous souhaitez refuser ou autoriser des paquets IP. Étant donné que vous sélectionnez ce qui se trouve à l'intérieur du paquet IP, vous refusez ou autorisez les paquets IP-in-IP.
- Les ACL de contrôleur ne peuvent pas bloquer l'adresse IP virtuelle du WLC, et donc les

paquets DHCP pour les clients sans fil.
- Les listes de contrôle d’accès ne peuvent pas bloquer le trafic de multidiffusion reçu des réseaux câblés destinés aux clients sans fil. Les listes de contrôle d'accès du contrôleur sont traitées pour le trafic de multidiffusion provenant de clients sans fil, destinés à des réseaux câblés ou à d'autres clients sans fil sur le même contrôleur.
- Contrairement à un routeur, la liste de contrôle d’accès contrôle le trafic dans les deux sens lorsqu’elle est appliquée à une interface, mais elle n’effectue pas de pare-feu dynamique. Si vous oubliez d’ouvrir un trou dans la liste de contrôle d’accès pour le trafic de retour, cela pose un problème.
- Les ACL de contrôleur bloquent uniquement les paquets IP. Vous ne pouvez pas bloquer des listes de contrôle d’accès de couche 2 ou des paquets de couche 3 qui ne sont pas IP.
- Les listes de contrôle d’accès des contrôleurs n’utilisent pas de masques inverses comme les routeurs. Ici, 255 signifie correspondre exactement à cet octet de l'adresse IP.
- Les listes de contrôle d’accès sur le contrôleur sont exécutées dans le logiciel et ont un impact sur les performances de transfert.

Remarque : si vous appliquez une liste de contrôle d'accès à une interface ou à un WLAN, le débit sans fil est dégradé et peut entraîner une perte potentielle de paquets. Afin d'améliorer le débit, supprimez la liste de contrôle d'accès de l'interface ou du WLAN et déplacez la liste de contrôle d'accès vers un périphérique câblé voisin.

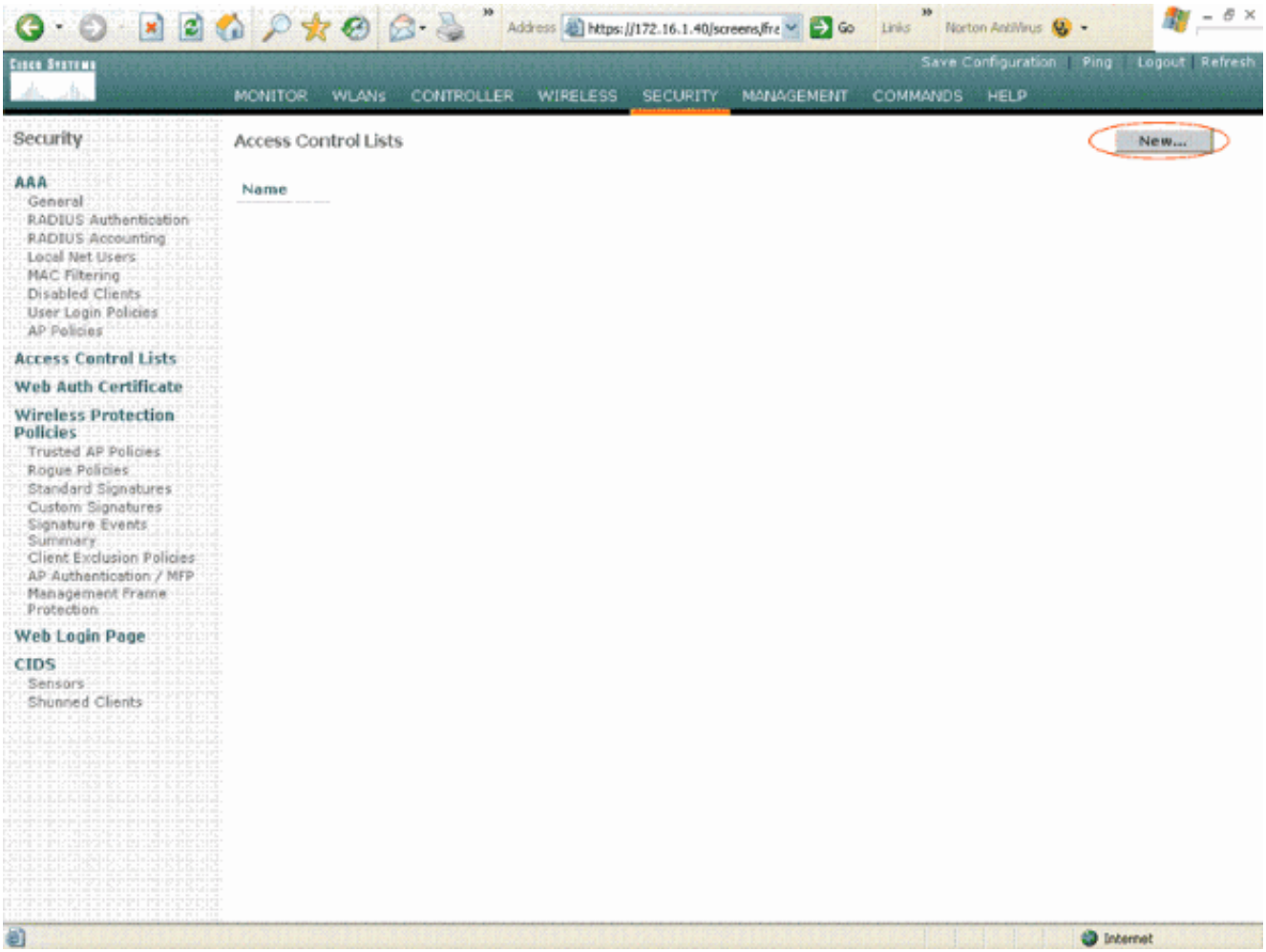
Configurer une ACL sur les WLC

Cette section décrit comment configurer une liste de contrôle d'accès sur le WLC. L'objectif est de configurer une liste de contrôle d'accès qui permette aux clients invités d'accéder à ces services :

- Protocole DHCP (Dynamic Host Configuration Protocol) entre les clients sans fil et le serveur DHCP
- Protocole ICMP (Internet Control Message Protocol) entre tous les périphériques du réseau
- DNS (Domain Name System) entre les clients sans fil et le serveur DNS
- Établissez une connexion Telnet avec un sous-réseau spécifique

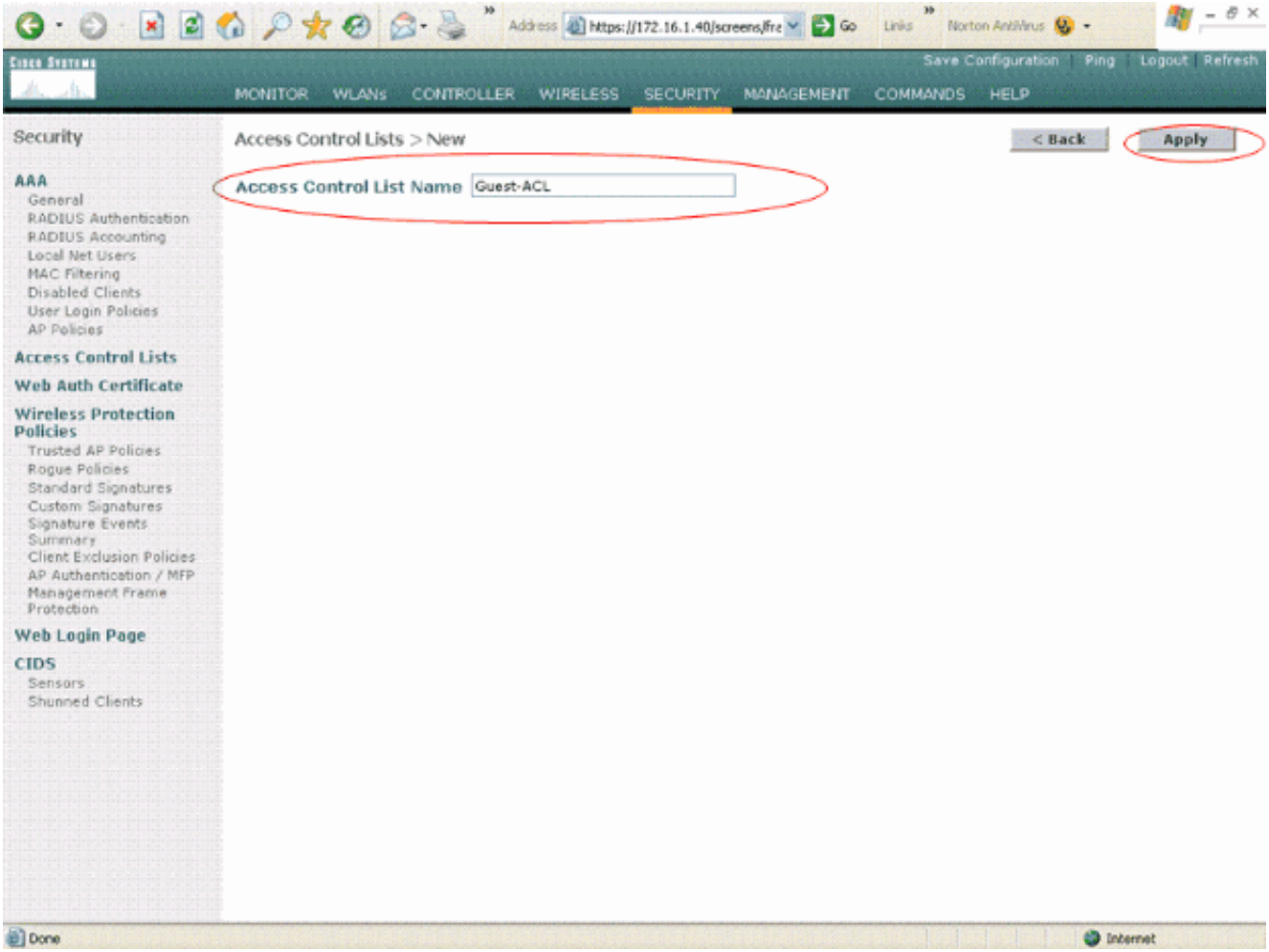
Tous les autres services doivent être bloqués pour les clients sans fil. Complétez ces étapes afin de créer l'ACL avec l'interface graphique du WLC :

1. Accédez à l'interface graphique utilisateur du WLC et choisissez **Security > Access Control Lists**.La page Listes de contrôle d'accès s'affiche. Cette page répertorie les ACL qui sont configurées sur le WLC. Elle vous permet également de modifier ou de supprimer les listes de contrôle d’accès. Afin de créer une nouvelle liste de contrôle d'accès, cliquez sur **Nouveau**
.



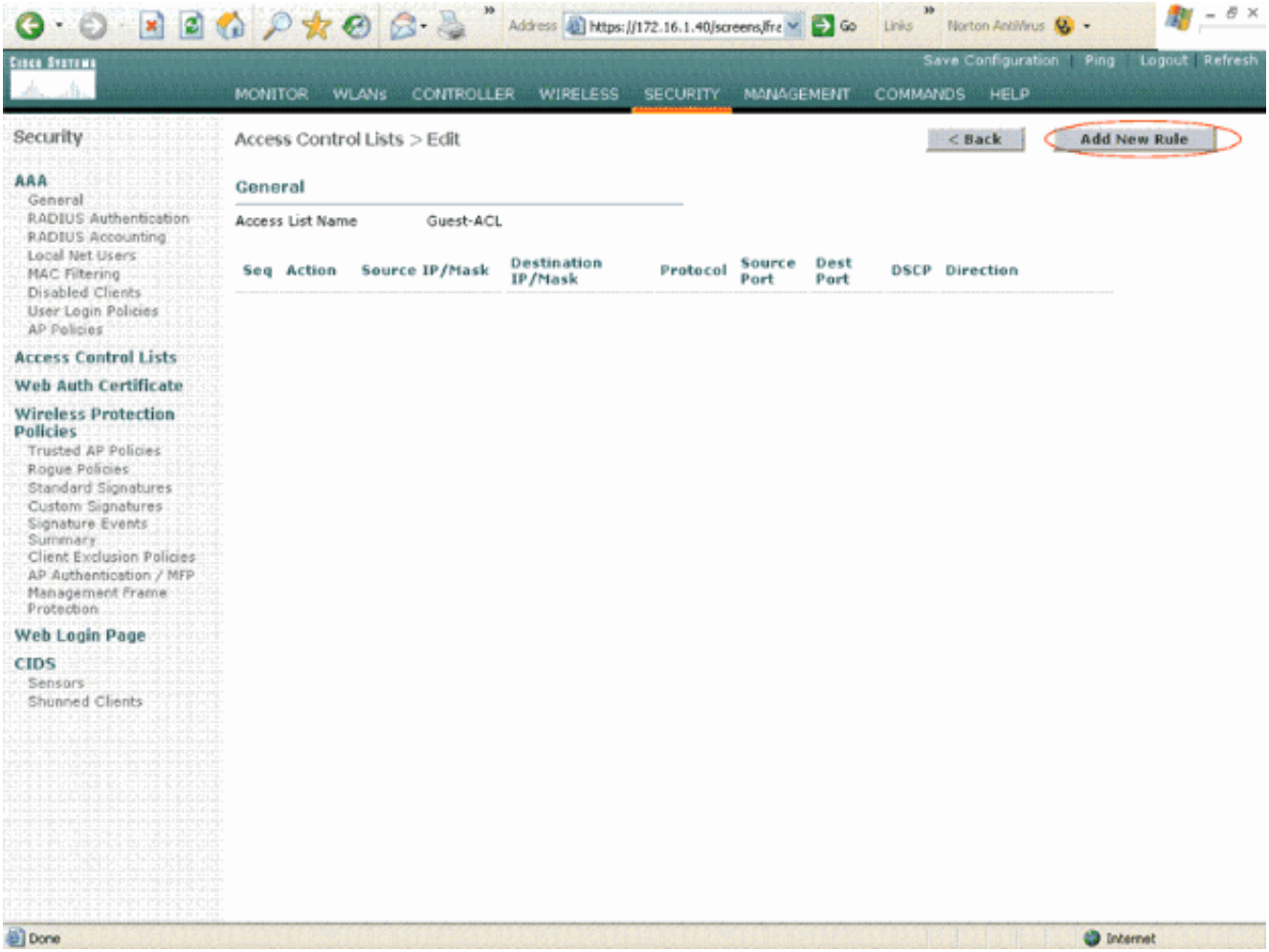
Listes de contrôle d'accès

2. Entrez le nom de la liste de contrôle d’accès et cliquez sur **Apply**.Vous pouvez entrer jusqu'à 32 caractères alphanumériques. Dans cet exemple, le nom de la liste de contrôle d'accès est **Guest-ACL** . Une fois la liste de contrôle d’accès créée, cliquez sur **Modifier** pour créer des règles pour la
liste.



Saisissez le nom de la liste de contrôle d'accès

3. Lorsque la page Listes de contrôle d'accès > Modifier apparaît, cliquez sur **Ajouter une nouvelle règle**.La page Listes de contrôle d'accès > Règles > Nouveau s'affiche.



Ajouter de nouvelles règles ACL

4. Configurez les règles qui autorisent un utilisateur invité à utiliser les services suivants :DHCP entre les clients sans fil et le serveur DHCPICMP entre tous les périphériques du réseauDNS entre les clients sans fil et le serveur DNSÉtablissez une connexion Telnet avec un sous-réseau spécifique

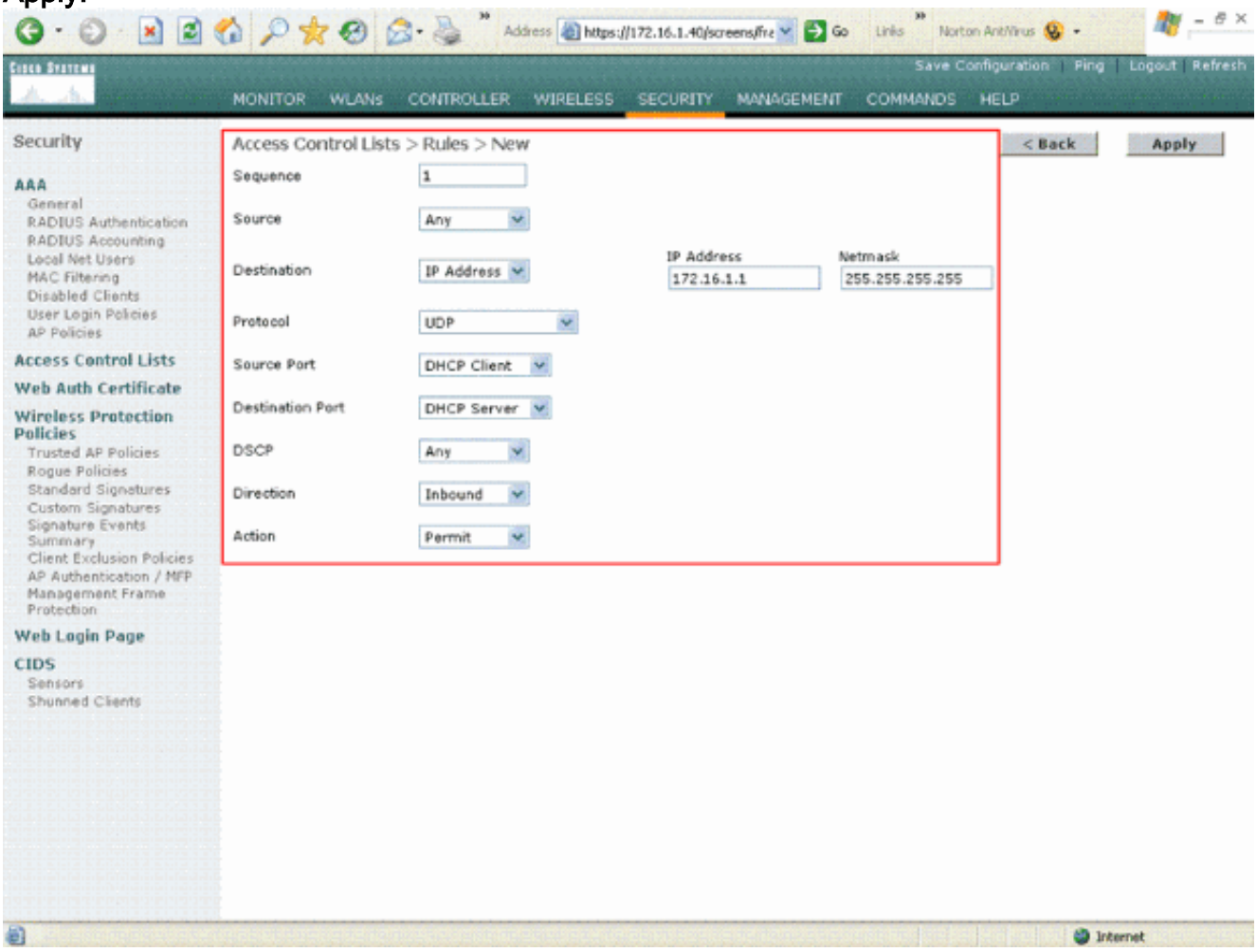
Configurer des règles autorisant les services d'utilisateur invité

Cette section présente un exemple de configuration des règles pour ces services :

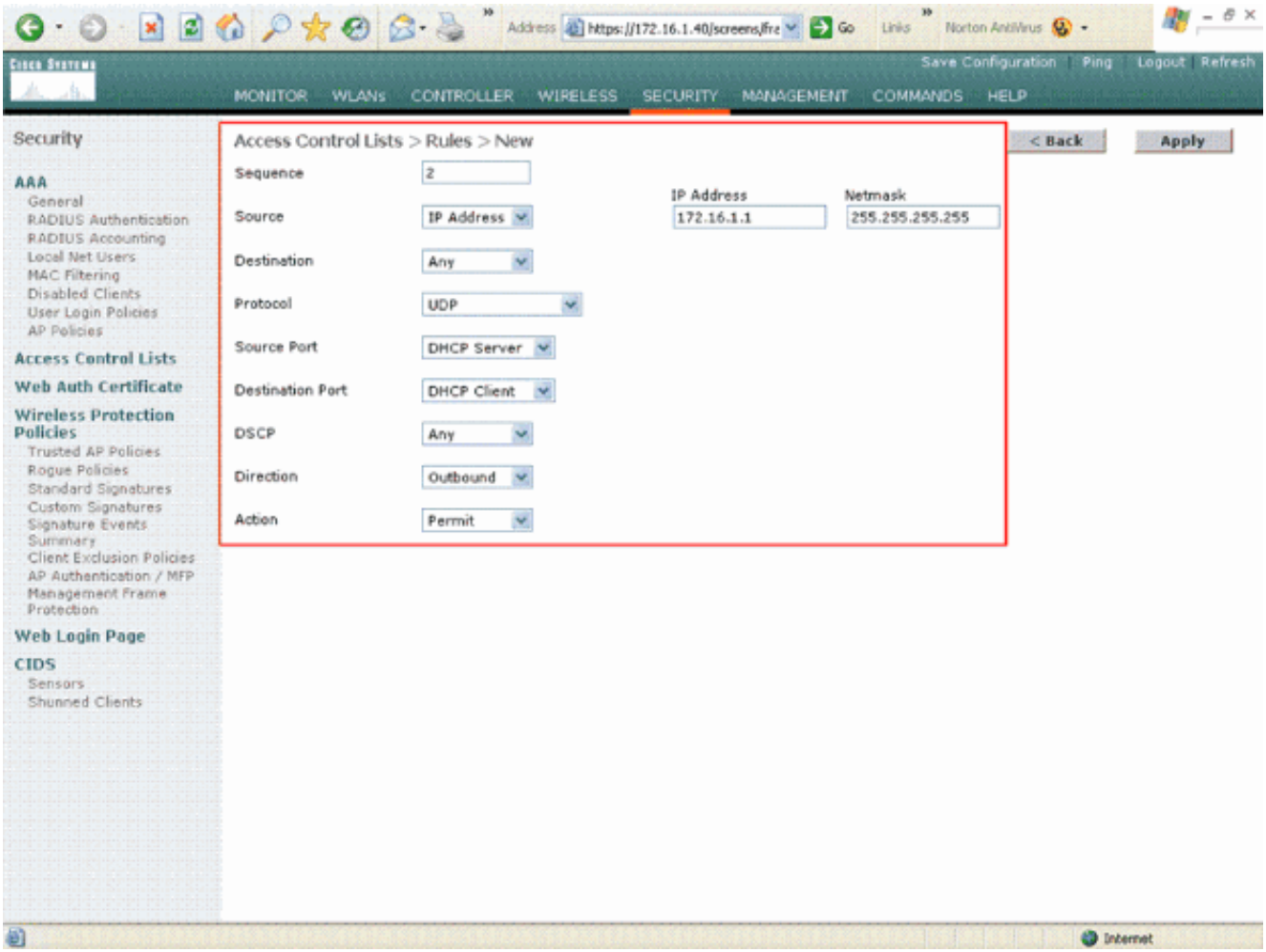
- DHCP entre les clients sans fil et le serveur DHCP
- ICMP entre tous les périphériques du réseau
- DNS entre les clients sans fil et le serveur DNS
- Établissez une connexion Telnet avec un sous-réseau spécifique

1. Afin de définir la règle pour le service DHCP, sélectionnez les plages IP source et de destination.Cet exemple utilise **any** pour la source, ce qui signifie qu'un client sans fil est autorisé à accéder au serveur DHCP. Dans cet exemple, le serveur 172.16.1.1 agit en tant que serveur DHCP et DNS. Ainsi, l'adresse IP de destination est 172.16.1.1/255.255.255.255 (avec un masque d'hôte).Comme DHCP est un protocole basé sur UDP, sélectionnez **UDP** dans le champ déroulant Protocol. Si vous avez choisi TCP ou UDP à l'étape précédente, deux paramètres supplémentaires apparaissent : Port source et Port de destination. Spécifiez les détails des ports source et de destination. Pour cette règle, le port source est le **client DHCP** et le port de destination est le **serveur DHCP** .Sélectionnez la direction dans laquelle la liste de contrôle d'accès doit être appliquée. Comme cette règle

s'applique du client au serveur, cet exemple utilise le **trafic entrant**. Dans la liste déroulante Action, sélectionnez **Permit** pour que cette liste de contrôle d'accès autorise les paquets DHCP du client sans fil vers le serveur DHCP. La valeur par défaut est Deny. Cliquez sur **Apply.**

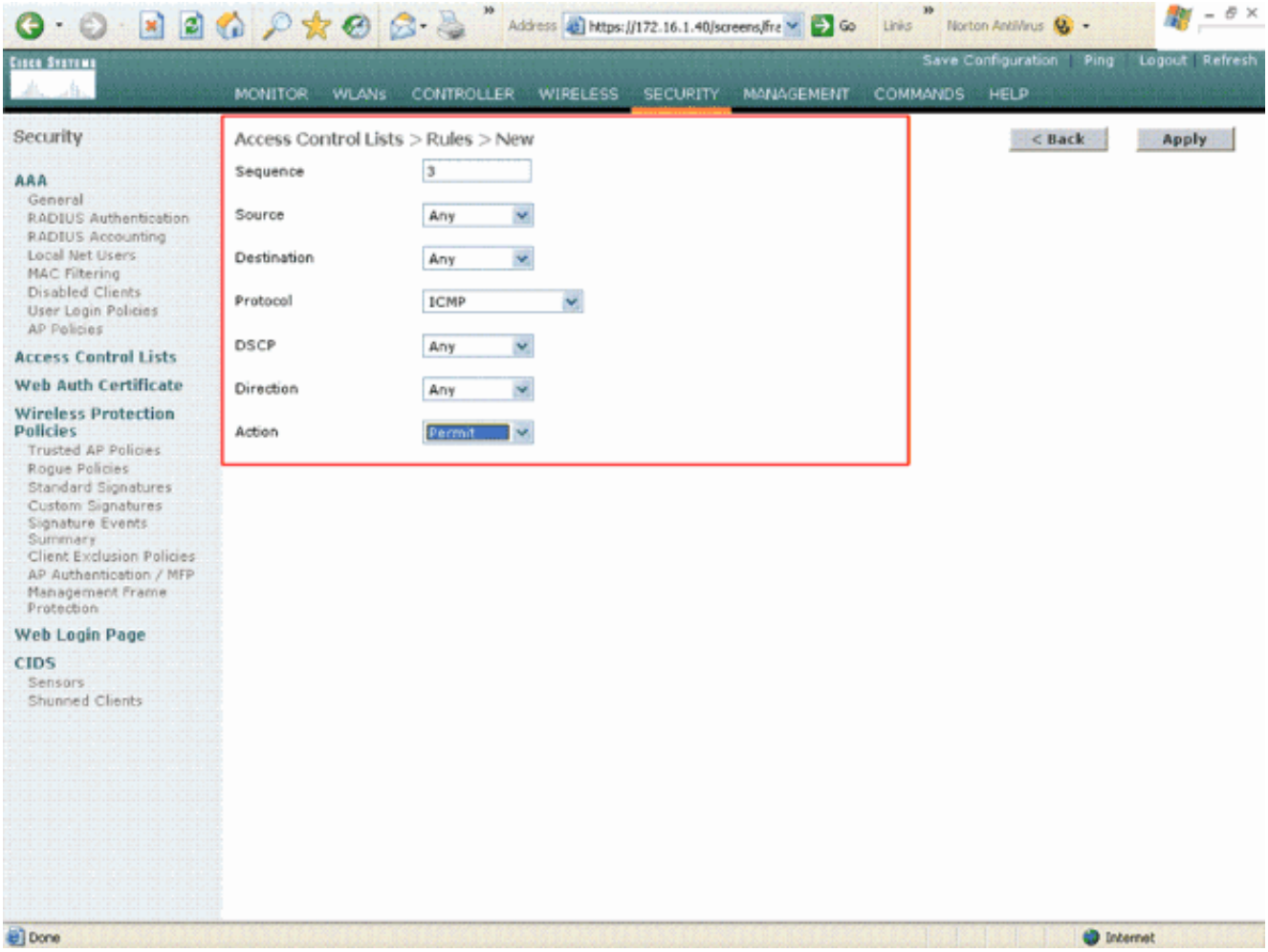


Sélectionnez Permit to Cause ACL to Allow DHCP Packets Si la source ou la destination n'**existe** pas, une instruction inverse dans la direction opposée doit être créée. Voici un exemple.



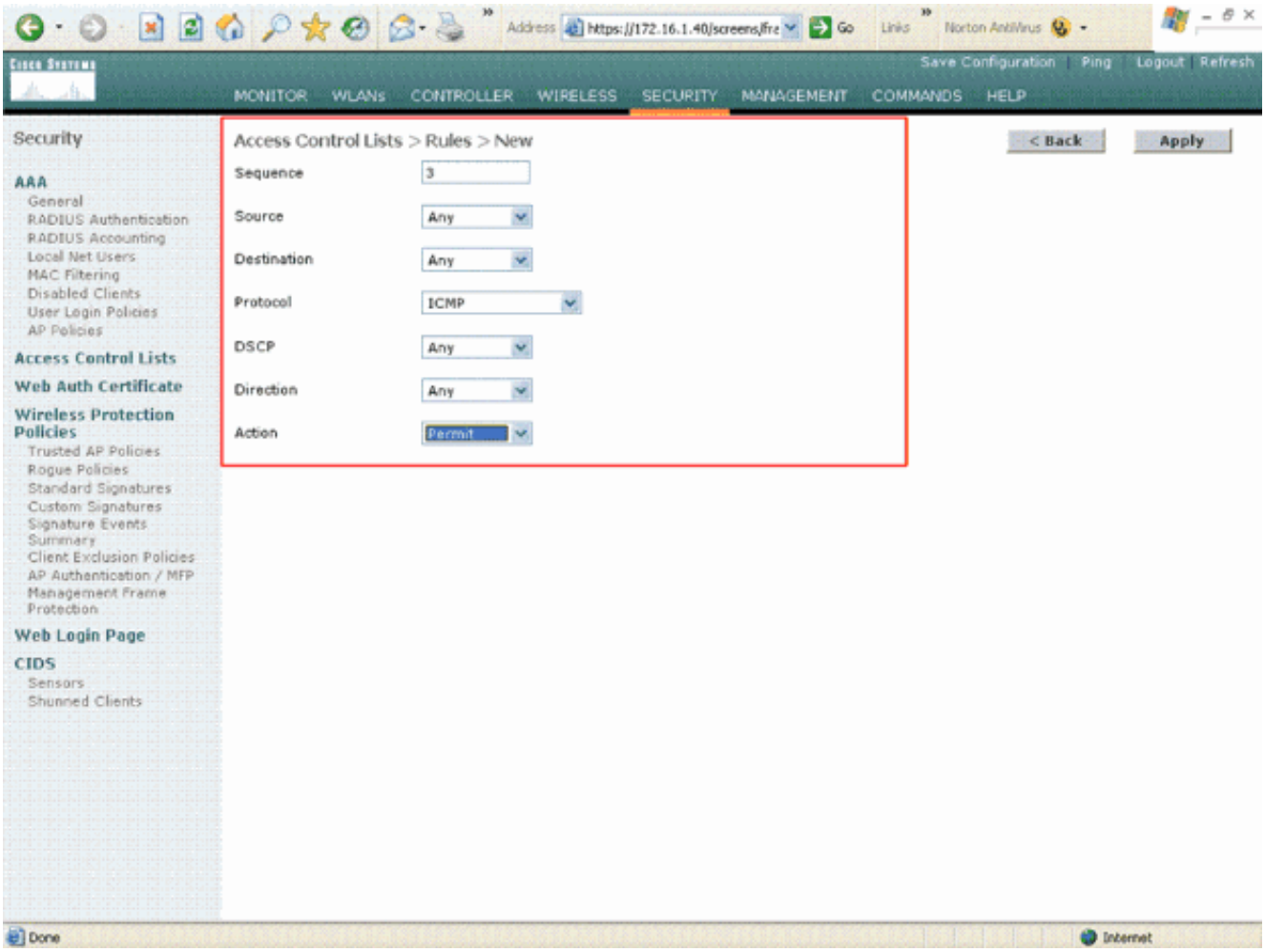
Source ou destination définie sur Any

2. Afin de définir une règle qui autorise les paquets ICMP entre tous les périphériques, sélectionnez **any** pour les champs Source et Destination. C'est la valeur par défaut.Choisissez **ICMP** dans le champ déroulant Protocol. Étant donné que cet exemple utilise **any** pour les champs Source et Destination, vous n'avez pas besoin de spécifier la direction. Il peut être conservé avec sa valeur par défaut **any** . En outre, l'instruction inverse dans la direction opposée n'est pas nécessaire.Dans le menu déroulant Action, choisissez **Permit** afin de faire en sorte que cette ACL autorise les paquets DHCP du serveur DHCP vers le client sans fil. Cliquez sur
Apply.

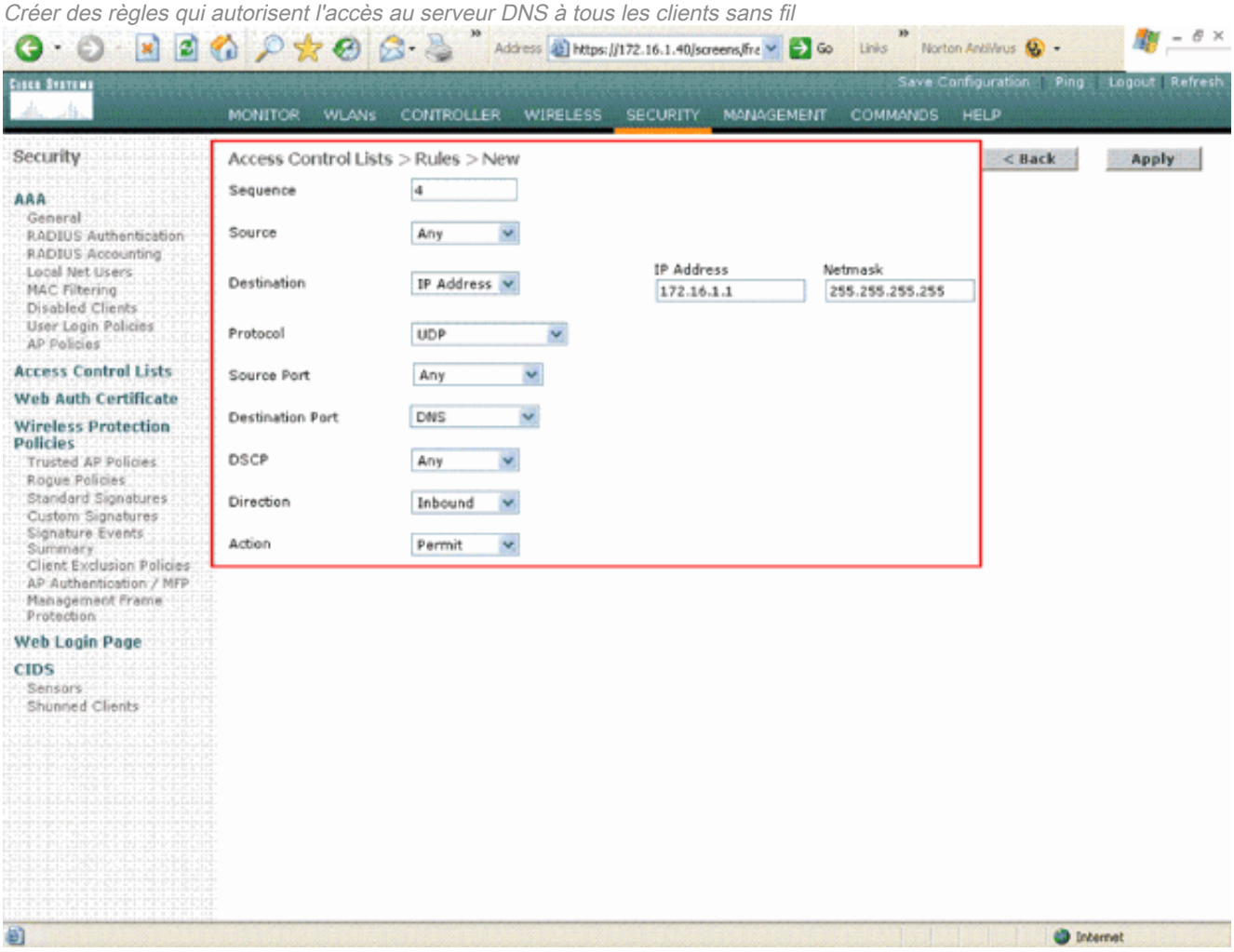


Autoriser à amener la liste de contrôle d'accès à autoriser les paquets DHCP du serveur DHCP vers le client sans fil

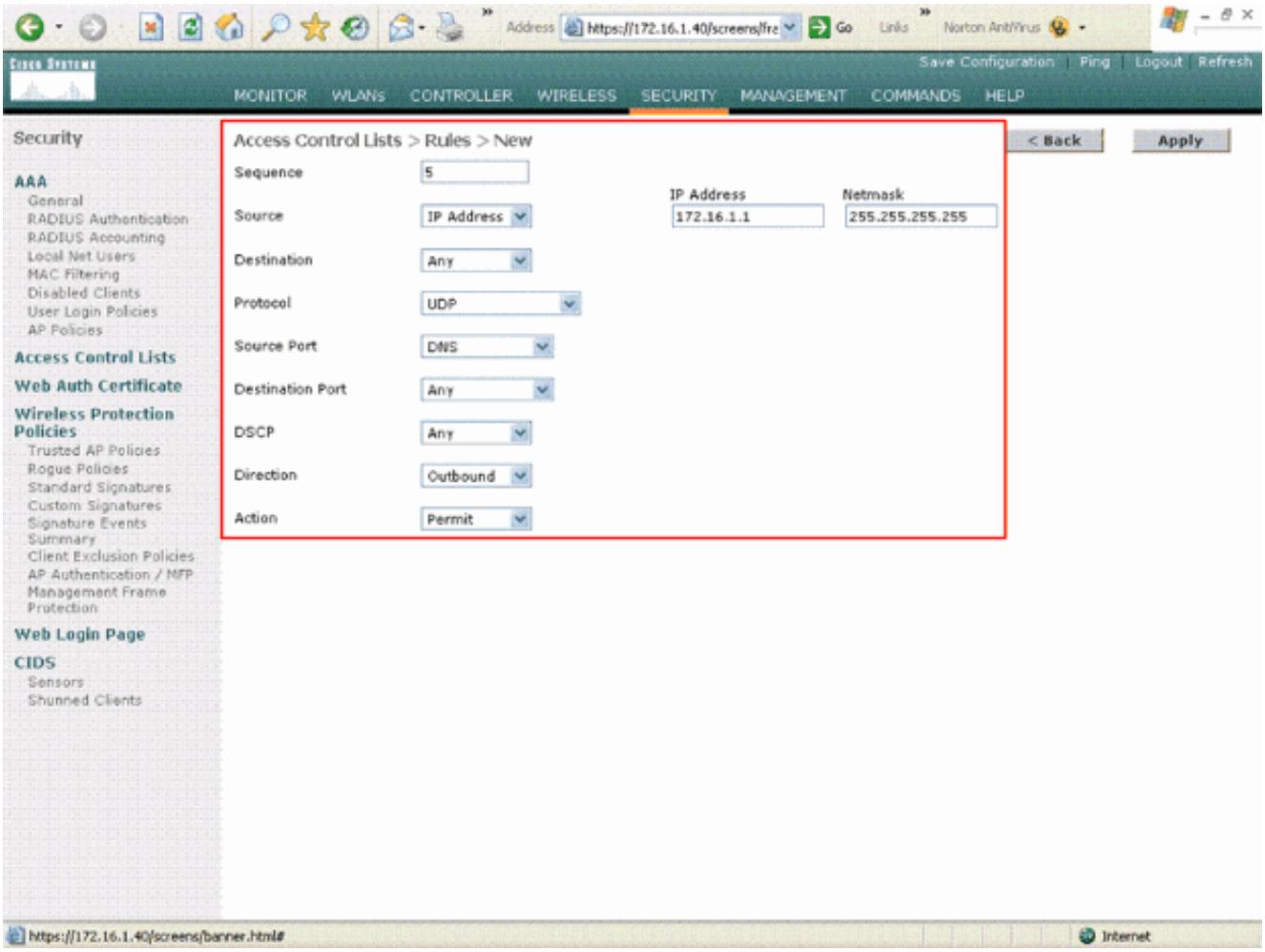
3. De même, créez des règles qui autorisent l'accès du serveur DNS à tous les clients sans fil et l'accès du serveur Telnet pour le client sans fil à un sous-réseau spécifique. Voici les exemples.



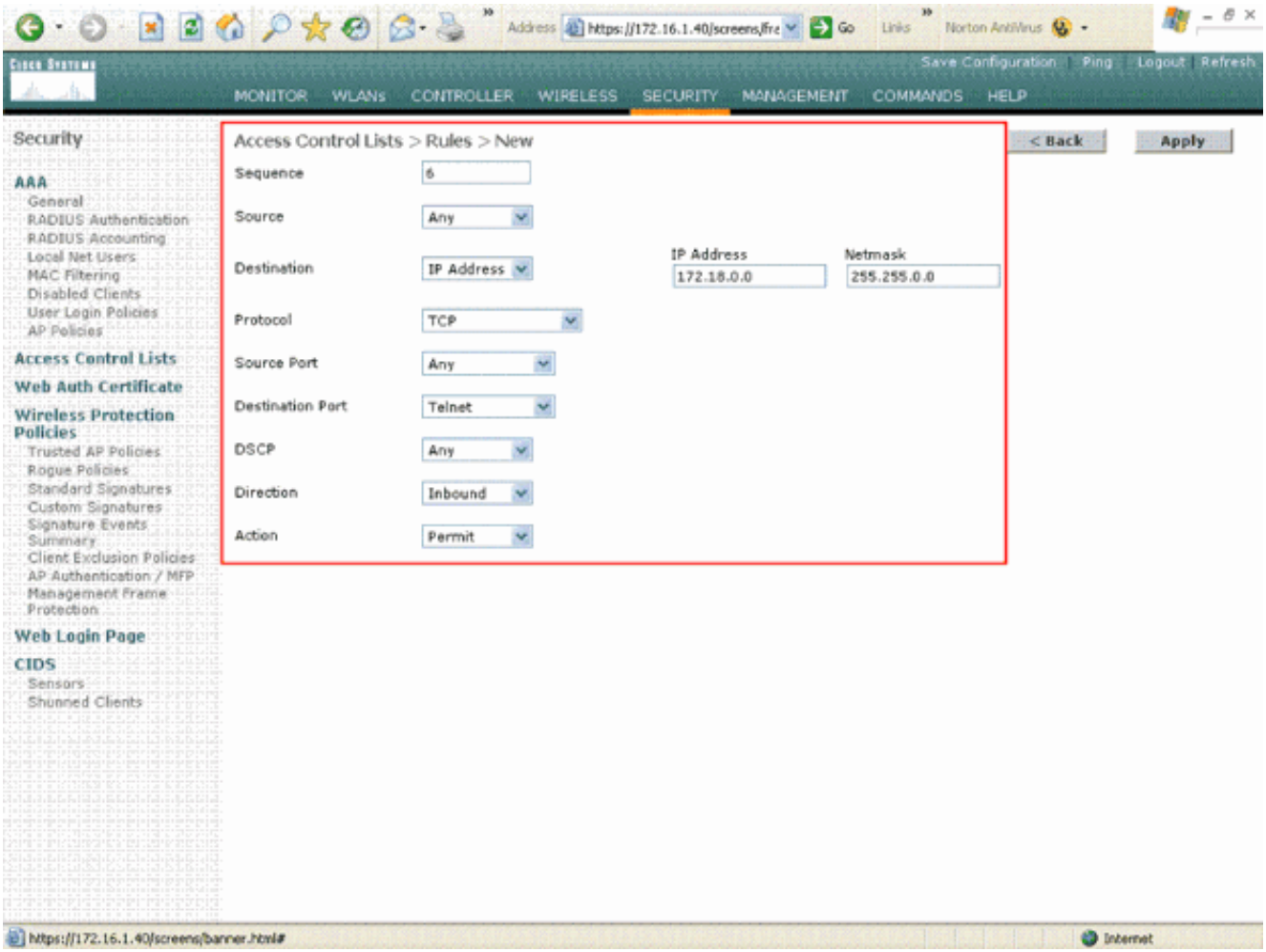
Créer des règles qui autorisent l'accès au serveur DNS à tous les clients sans fil



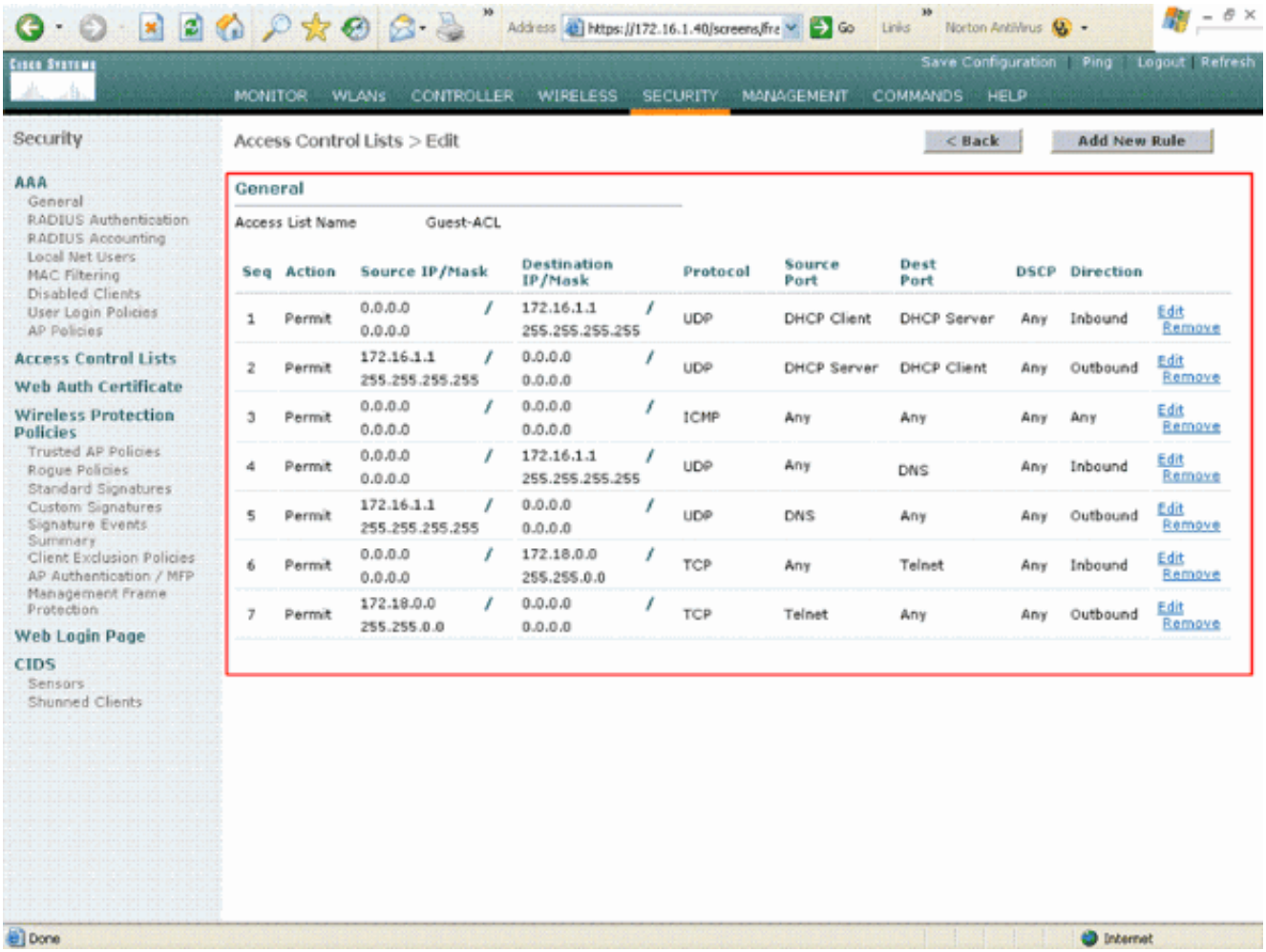
Créer des règles autorisant l'accès du serveur Telnet pour le client sans fil à un sous-réseau Définissez cette règle afin d'autoriser l'accès du client sans fil au service Telnet.



Autoriser l'accès du client sans fil au service Telnet

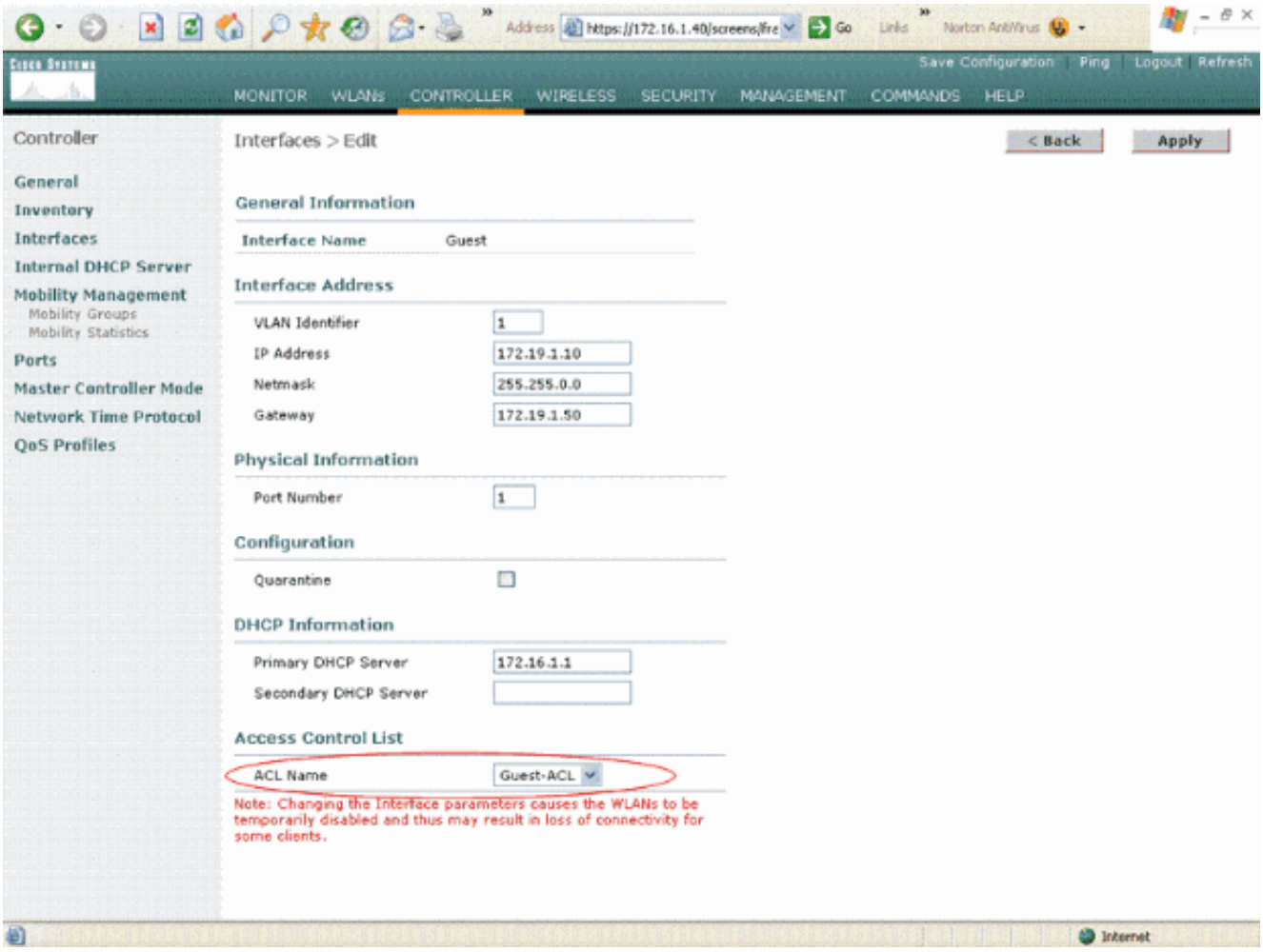


Autre exemple d'accès client sans fil au service Telnet La page **ACL > Edit** répertorie toutes les règles définies pour la liste de contrôle d'accès.



La page Edit répertorie toutes les règles définies pour la liste de contrôle d'accès

4. Une fois créée, la liste de contrôle d’accès doit être appliquée à une interface dynamique. Afin d'appliquer l'ACL, choisissez **Controller > Interfaces** et modifiez l'interface à laquelle vous voulez appliquer l'ACL.
5. Dans la page **Interfaces > Edit** pour l'interface dynamique, choisissez la liste de contrôle d'accès appropriée dans le menu déroulant Access Control Lists. Voici un exemple.



Sélectionnez la liste de contrôle d'accès appropriée dans le menu Access Control List

Une fois cette opération effectuée, la liste de contrôle d'accès autorise et refuse le trafic (en fonction des règles configurées) sur le WLAN qui utilise cette interface dynamique. La liste de contrôle d'accès d'interface peut uniquement être appliquée aux AP H-Reap en mode connecté, mais pas en mode autonome.

> **Remarque** : ce document suppose que les WLAN et les interfaces dynamiques sont configurés. Référez-vous à Configurer des VLAN sur des contrôleurs LAN sans fil ou aux informations sur la façon de créer des interfaces dynamiques sur des WLC.

Configurer les ACL du processeur

Auparavant, les ACL sur les WLC n'avaient pas d'option pour filtrer le trafic de données LWAPP/CAPWAP, le trafic de contrôle LWAPP/CAPWAP et le trafic de mobilité destiné aux interfaces de gestion et de gestionnaire d'AP. Afin de résoudre ce problème et de filtrer le trafic LWAPP et de mobilité, des ACL de CPU ont été introduites avec la version 4.0 du microprogramme WLC.

La configuration des listes de contrôle d'accès du processeur comprend deux étapes :

1. Configurez les règles pour la liste de contrôle d'accès CPU.
2. Appliquez la liste de contrôle d'accès du processeur sur le WLC.

Les règles de la liste de contrôle d'accès du processeur doivent être configurées de la même manière que les autres listes de contrôle d'accès.

Vérifier

Cisco vous recommande de tester vos configurations de liste de contrôle d'accès avec un client sans fil afin de vous assurer que vous les avez configurées correctement. S'ils ne fonctionnent pas correctement, vérifiez les listes de contrôle d'accès sur la page Web de la liste de contrôle d'accès et assurez-vous que vos modifications ont été appliquées à l'interface du contrôleur.

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

- **show acl summary** - Afin d'afficher les ACL qui sont configurées sur le contrôleur, utilisez la commande **show acl summary**.Voici un exemple :

```
(Cisco Controller) >show acl summary

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

- **show acl detailedACL_Name** : affiche des informations détaillées sur les ACL configurées.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** : pour afficher les listes de contrôle d'accès configurées sur le processeur, utilisez la commande **show acl cpu**.Voici un exemple :

```
(Cisco Controller) >show acl cpu

CPU Acl Name.............................. CPU-ACL
Wireless Traffic.......................... Enabled
Wired Traffic............................. Enabled
```

Dépannage

Le logiciel du contrôleur version 4.2.x ou ultérieure vous permet de configurer les compteurs de liste de contrôle d'accès. Les compteurs de listes de contrôle d’accès peuvent aider à déterminer quelles listes ont été appliquées aux paquets transmis par le contrôleur. Cette fonctionnalité est utile lorsque vous dépannez votre système.

Les compteurs ACL sont disponibles sur ces contrôleurs :

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

Pour activer cette fonction, procédez comme suit :

1. Choisissez **Security > Access Control Lists > Access Control Lists** afin d'ouvrir la page Access Control Lists.Cette page répertorie toutes les listes de contrôle d'accès qui ont été configurées pour ce contrôleur.
2. Afin de voir si des paquets atteignent l'une des ACL configurées sur votre contrôleur, cochez la case **Enable Counters** et cliquez sur **Apply**. Sinon, ne cochez pas cette case. C'est la valeur par défaut.
3. Si vous souhaitez effacer les compteurs d’une liste de contrôle d’accès, placez votre curseur sur la flèche bleue de la liste de contrôle d’accès et choisissez **Effacer les compteurs** .

Informations connexes

- Guide de configuration du contrôleur de LAN sans fil Cisco, version 6.0
- Configurer des VLAN sur des contrôleurs LAN sans fil
- Dépannage d’un point d’accès allégé qui ne parvient pas à se connecter à un WLC
- Assistance technique et téléchargements Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.