Wireless LAN Controller での ACL の設定例

目次

はじめに

このドキュメントでは、WLAN に着信または発信するトラフィックをフィルタリングするために、Wireless LAN Controller（WLC）上でアクセス コントロール リスト（ACL）を設定する方法を説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- WLC と Lightweight アクセス ポイント（LAP）の基本動作のための設定方法に関する知識
- Lightweight アクセス ポイント プロトコル（LWAPP）とワイヤレスのセキュリティ方式に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ファームウェア 4.0 を実行する Cisco 2000 シリーズ WLC
- Cisco 1000 シリーズ LAP
- ファームウェア 2.6 を実行する Cisco 802.11a/b/g ワイヤレス クライアント アダプタ
- Cisco Aironet Desktop Utility（ADU）バージョン 2.6

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

WLC 上の ACL

WLC 上の ACL は、WLAN 上でのワイヤレス クライアントへのサービスを制限または許可することを目的としています。

WLC ファームウェア バージョン 4.0 よりも前のバージョンでは、管理インターフェイスでは ACL を迂回しており、[Management Via Wireless] オプションを使用してワイヤレス クライアントによるコントローラの管理を禁止する以外に、WLC 宛てのトラフィックに影響を与えることができません。 したがって、ACL は、ダイナミック インターフェイスだけに適用できます。 WLC ファームウェア バージョン 4.0 には、管理インターフェイスを宛先としたトラフィックをフィルタリングできる、CPU ACL があります。 CPU ACL の設定方法の一例をこのドキュメントで後述してあります。

最大で 64 個の ACL を定義でき、各 ACL に最大 64 個のルール（またはフィルタ）を設定できます。 各ルールには、ルールの処理に影響を与えるパラメータがあります。 パケットが 1 つのルールの全パラメータと一致した場合、そのルールに設定されている処理がそのパケットに適用されます。 ACL は、GUI または CLI のいずれかを使用して設定できます。

WLC 上の ACL を設定する前に理解する必要のある複数のルールを次に示します。

- 送信元*および*宛先が **any** の場合は、この ACL を適用する方向に **any** を指定できます。
- 送信元と宛先の*いずれか*が **any でない**場合は、フィルタの方向を指定する必要があり、反対方向の inverse ステートメントを作成する必要があります。
- WLC での着信と発信の概念は、直接的ではありません。 クライアントからの視点ではなく、ワイヤレス クライアントと接している WLC を中心とした視点です。 したがって、着信方向は、ワイヤレス クライアントから WLC に着信するパケットを意味し、発信方向は、WLC からワイヤレス クライアントに向けて発信されるパケットを意味します。
- ACL の末尾には、暗黙的な deny があります。

WLC に ACL を設定するときの考慮事項

WLC 内の ALC は、ルータ内とは異なる働きをします。 WLC 内の ACL を設定するときに留意する必要のある事項を次に示します。

- IP パケットを拒否または許可しようとする場合、最も誤りやすい部分は、IP の選択です。 IP パケットに含まれる情報を選択することになるため、結局は、IP-in-IP パケットを拒否または許可することになります。
- コントローラ ACL では、1.1.1.1（仮想 IP アドレス）をブロックできず、したがってワイヤレス クライアントのための DHCP パケットをブロックできません。
- コントローラ ACL は有線ネットワークから受信される無線クライアントに向かうマルチキャ

ストトラフィックをブロックできません。 コントローラ ACL は同じコントローラの有線ネットワークか他の無線クライアントに向かう無線クライアントから初期化されるマルチキャストトラフィックのために処理されます。
- ACL をインターフェイスに適用した場合、ルータとは異なり、両方向のトラフィックを制御しますが、ステートフル ファイアウォール処理は実行されません。 トラフィックを戻すための穴を ACL に開け忘れると、問題が生じます。
- コントローラ ACL では、IP パケットのみをブロックします。 レイヤ 2 ACL や、IP ではないレイヤ 3 パケットはブロックできません。
- コントローラ ACL では、ルータなどの逆マスクを使用しません。 ここで、255 は、IP アドレスの該当オクテットが完全に一致していることを意味します。
- コントローラ上の ACL はソフトウェア内で実施され、転送パフォーマンスに影響します。

注: インターフェイスまたは WLAN に ACL を適用すると、ワイヤレス スループットの低下からパケットの損失につながるおそれがあります。 スループットを向上させるには、インターフェイスまたは WLAN から ACL を削除し、ネイバー有線デバイスにこの ACL を移動します。

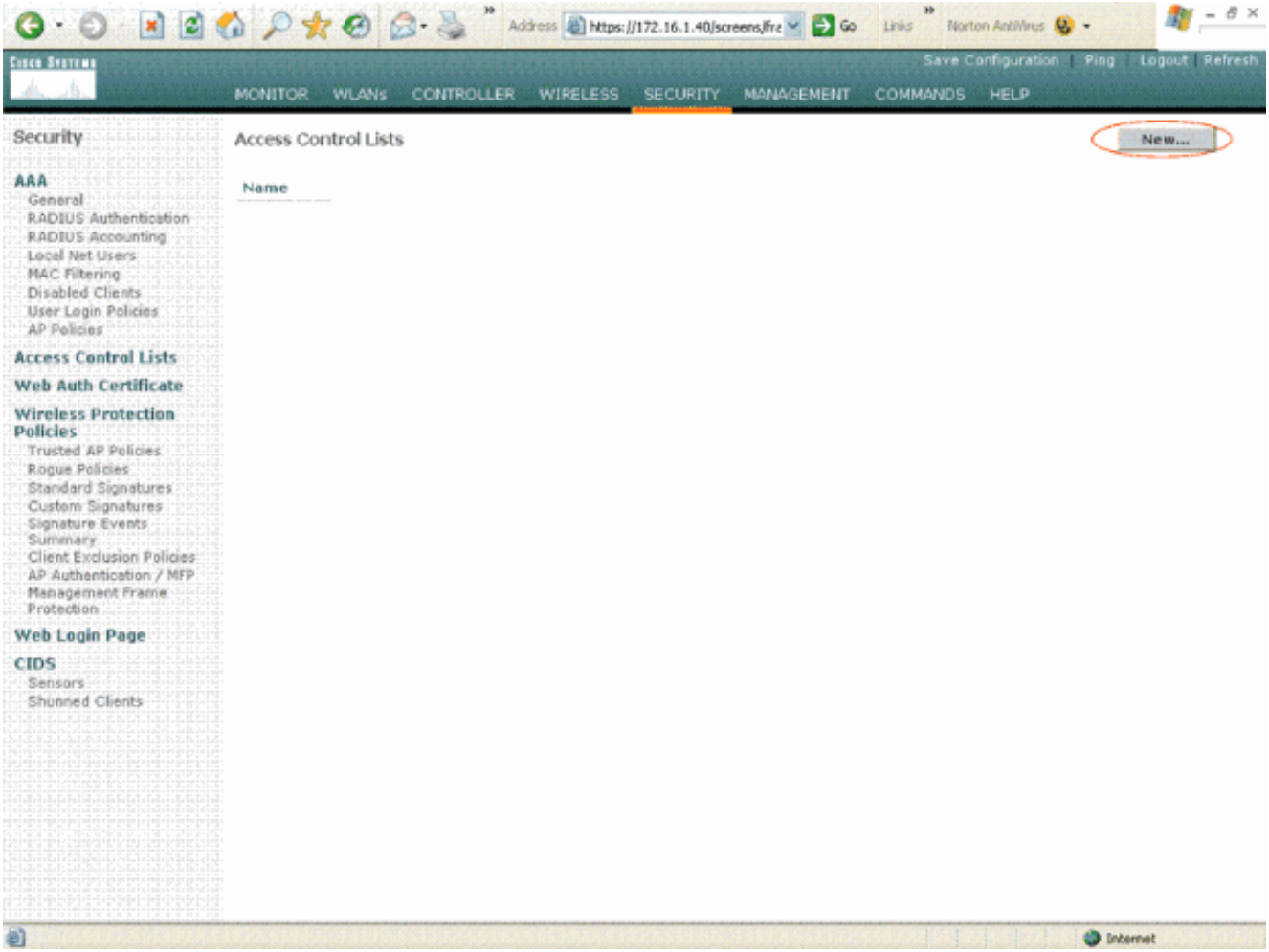
WLC 上の ACL の設定

この項では、WLC 上での ACL の設定方法について説明します。 以下のサービスへのアクセスをゲスト クライアントに許可するように ACL を設定することを目的とします。

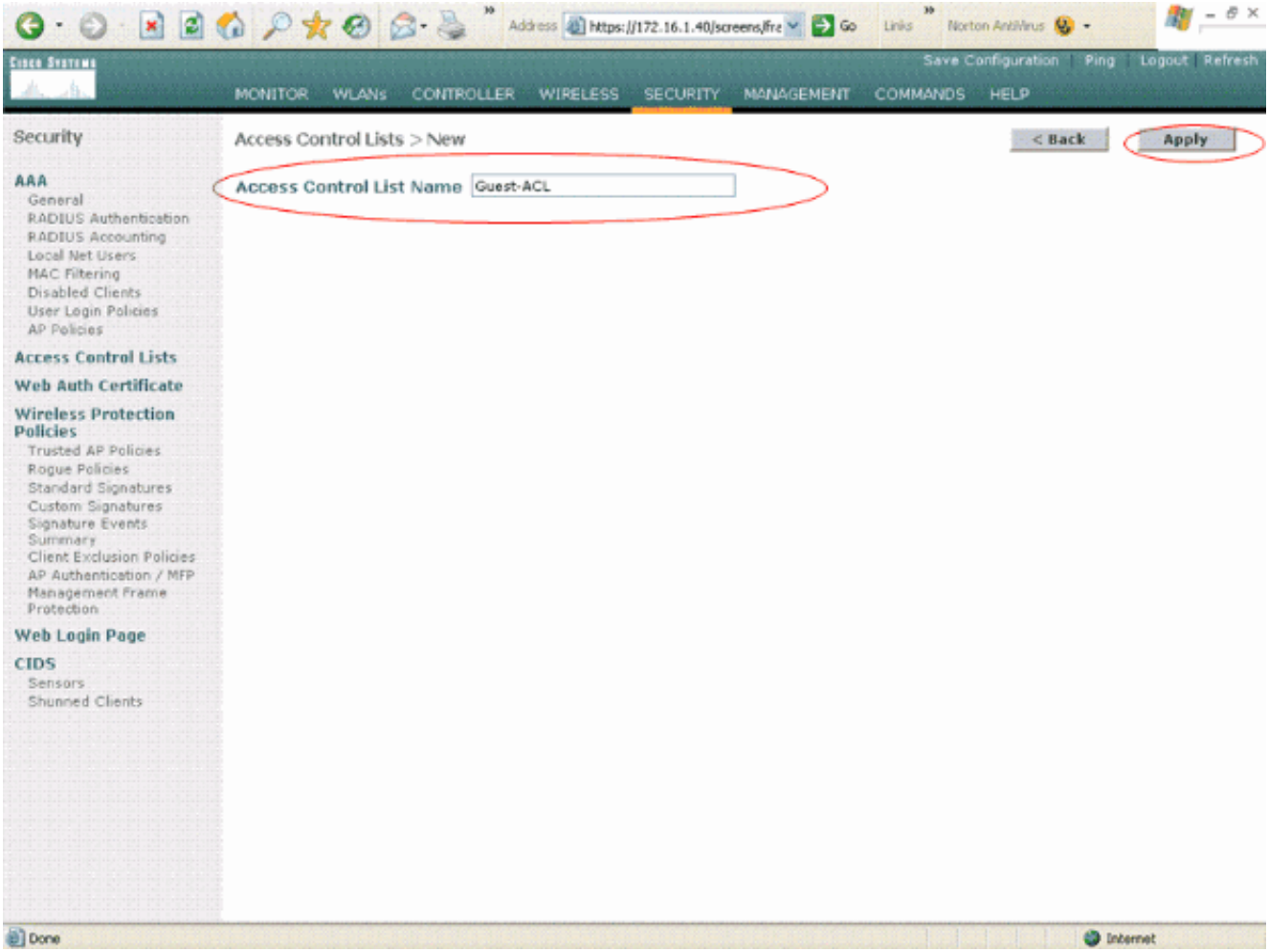
- ワイヤレス クライアントと DHCP サーバの間のダイナミック ホスト コンフィギュレーション プロトコル（DHCP）
- ネットワーク内の全デバイス間のインターネット制御メッセージ プロトコル（ICMP）
- ワイヤレス クライアントと DNS サーバの間のドメイン ネーム システム（DNS）
- 特定のサブネットへの Telnet

このワイヤレス クライアントに対する他のすべてのサービスはブロックされる必要があります。WLC GUI を使用して ACL を作成するには、次の手順を実行します。

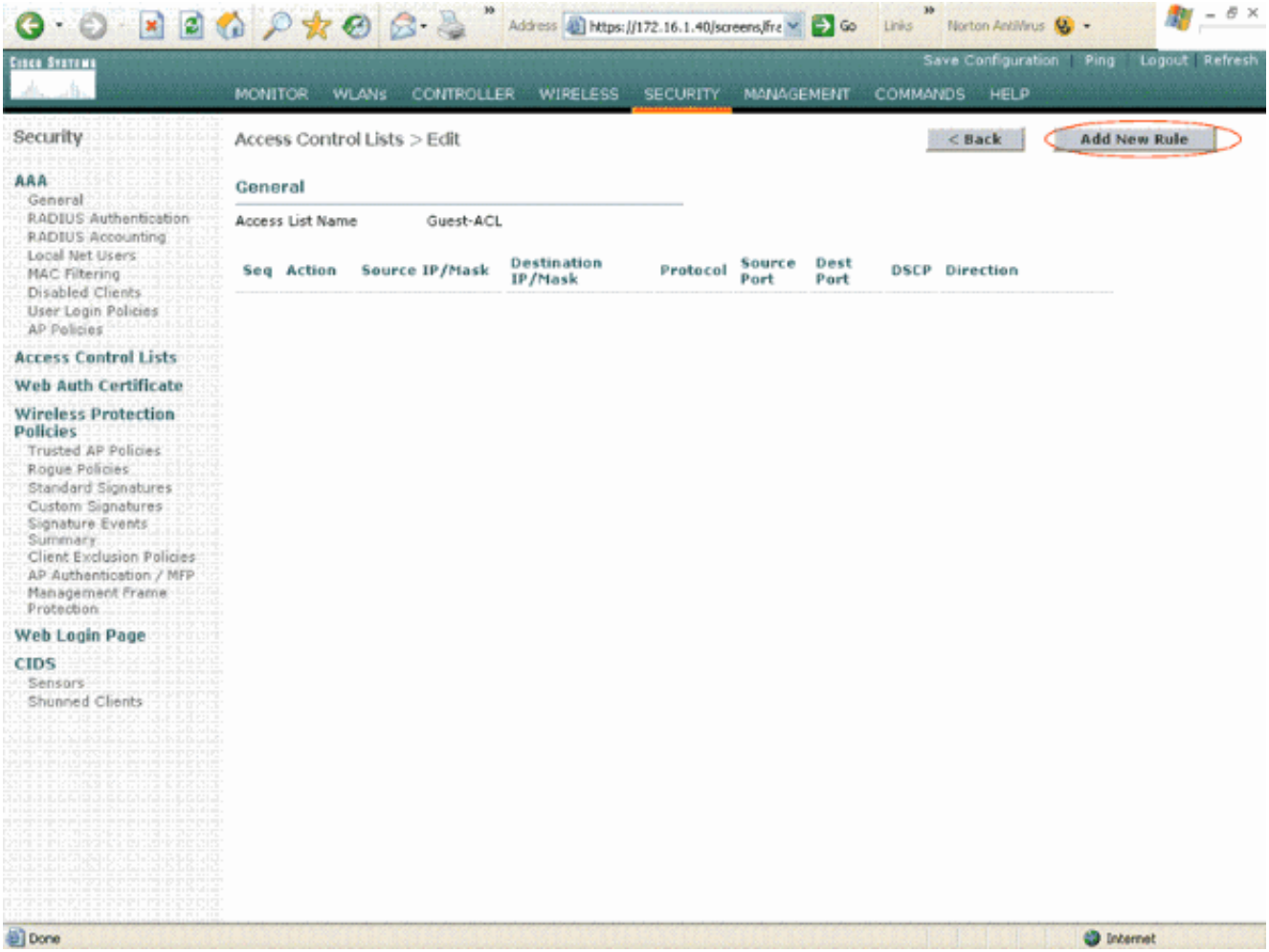
1. WLC GUI に移動し、[Security] > [Access Control Lists] を選択します。[Access Control Lists] ページが表示されます。 このページには、WLC に設定されている ACL の一覧が表示されます。 任意の ACL を編集または削除することもできます。 新しい ACL を作成するには、[New] をクリックします。



2. ACL の名前を入力し、[Apply] をクリックします。最大 32 文字の英数字を入力できます。この例では、ACL の名前は **Guest-ACL** です。 ACL が作成されたら、この ACL のルールを作成するために [Edit] をクリックします。



3. [Access Control Lists > Edit] ページが表示されたら、[Add New Rule] をクリックします。[Access Control Lists > Rules > New] ページが表示されます。



4. ゲスト ユーザに次のサービスを許可するルールを設定します。ワイヤレス クライアントと DHCP サーバの間の DHCPネットワーク内の全デバイス間の ICMPワイヤレス クライアントと DNS サーバの間の DNS特定のサブネットへの Telnet

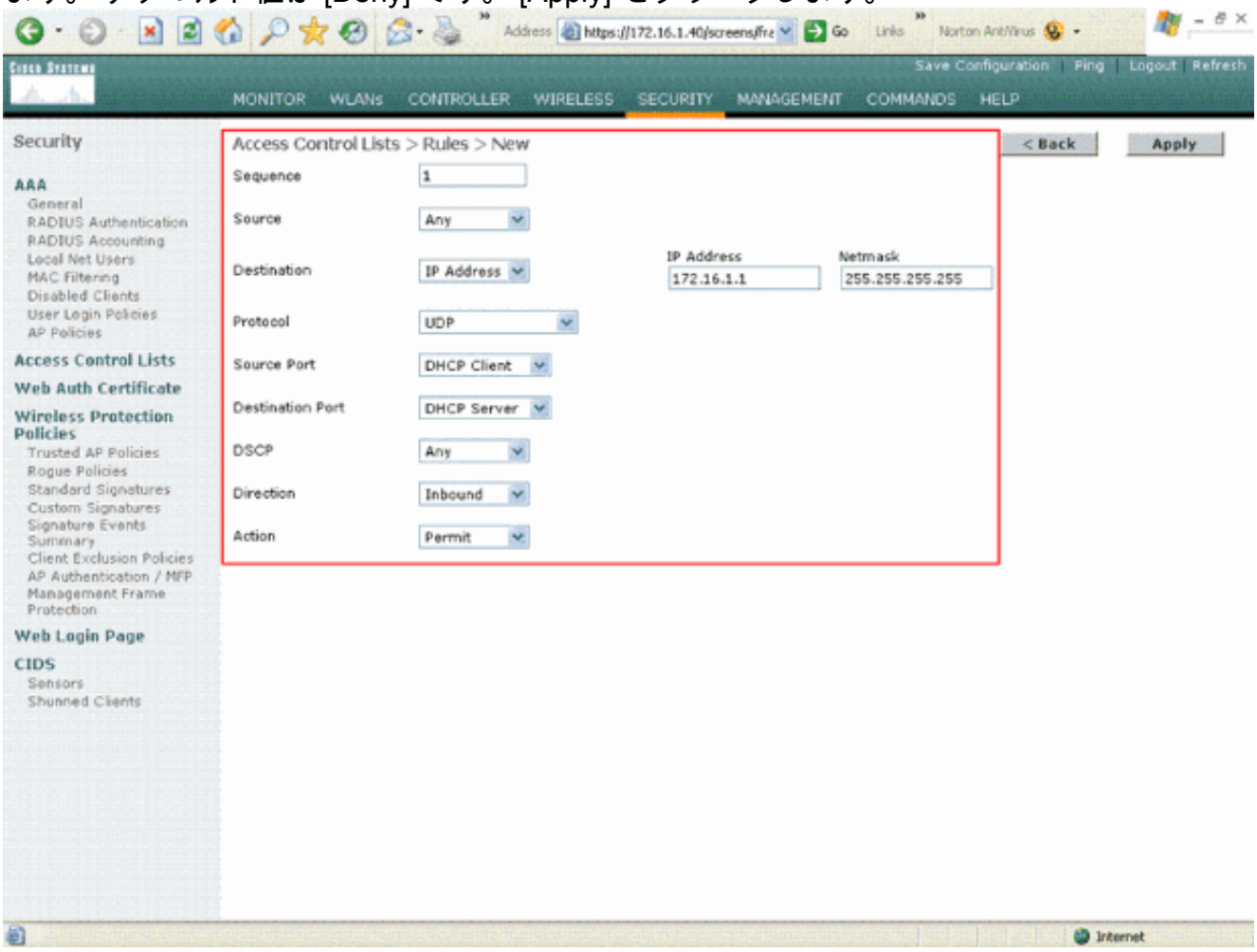
ゲスト ユーザ サービスを可能にするルールの設定

ここでは、次のサービスに対するルールの設定方法の一例を示します。

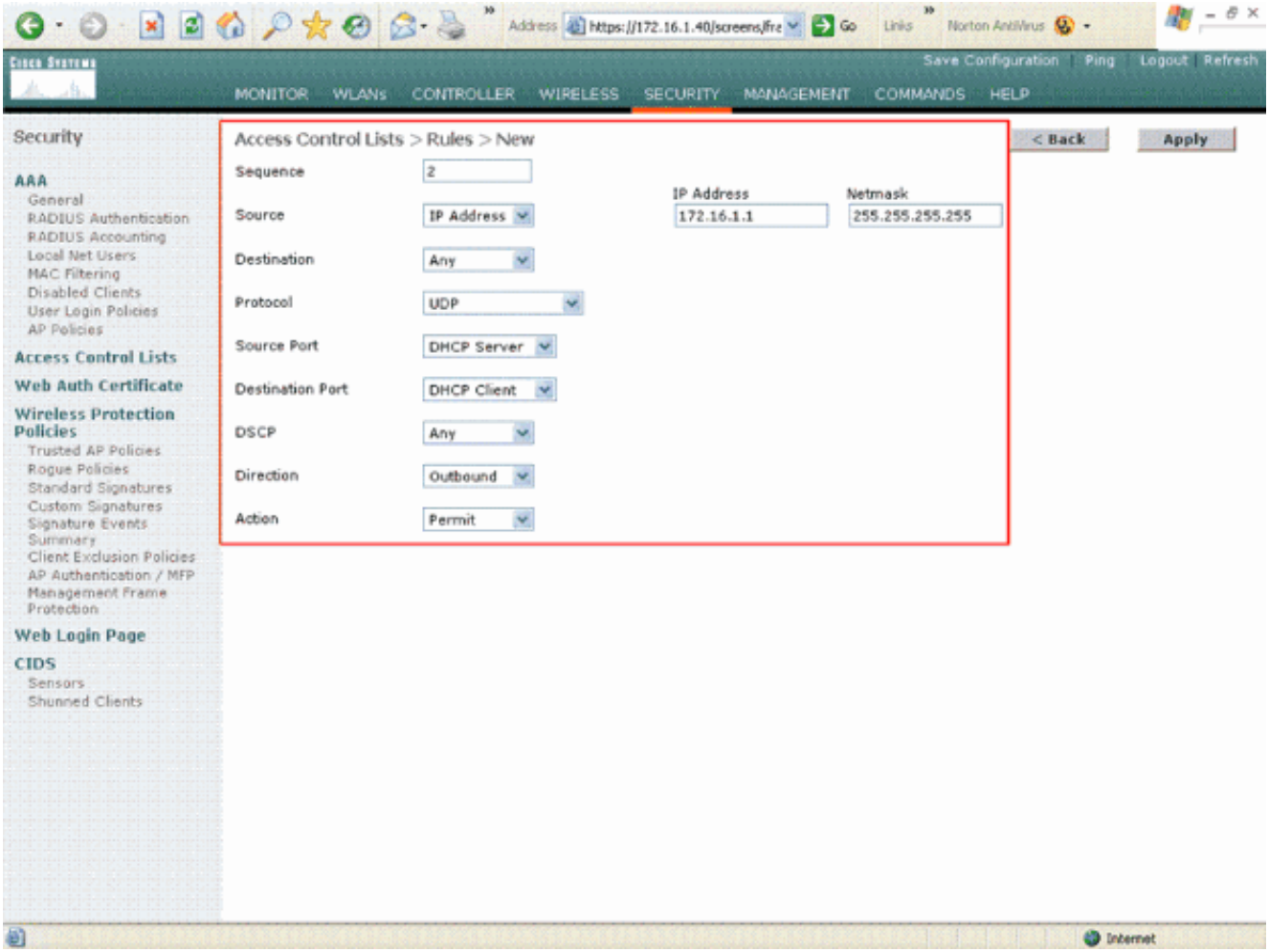
- ワイヤレス クライアントと DHCP サーバの間の DHCP
- ネットワーク内の全デバイス間の ICMP
- ワイヤレス クライアントと DNS サーバの間の DNS
- 特定のサブネットへの Telnet

1. DHCP サービスのルールを定義するために、送信元および宛先の IP 範囲を選択します。この例では、すべてのワイヤレス クライアントに DHCP サーバへのアクセスを許可する **any** を送信元に使用します。 この例では、サーバ 172.16.1.1 が DHCP サーバおよび DNS サーバとして機能します。 したがって、宛先 IP アドレスは 172.16.1.1/255.255.255.255 (ホスト マスク付き) です。DHCP は UDP ベースのプロトコルであるため、[Protocol] ドロップダウン フィールドから [UDP] を選択します。 前のステップで TCP または UDP を選択した場合は、追加で 2 個のパラメータが表示されます。 [Source Port] および [Destination Port] です。 送信元ポートおよび宛先ポートの詳細を指定します。 このルールの場合、送信元ポートは [DHCP Client]、宛先ポートは [DHCP Server] です。ACL を適用する方向を選択します。 このルールは、クライアントからサーバへのルールであるため、この例では [Inbound] を使用します。 [Action] ドロップダウン ボックスで、[Permit] を選択して、ワイヤレス クライアントから DHCP サーバへの DHCP パケットがこの ACL によって許可されるようにし

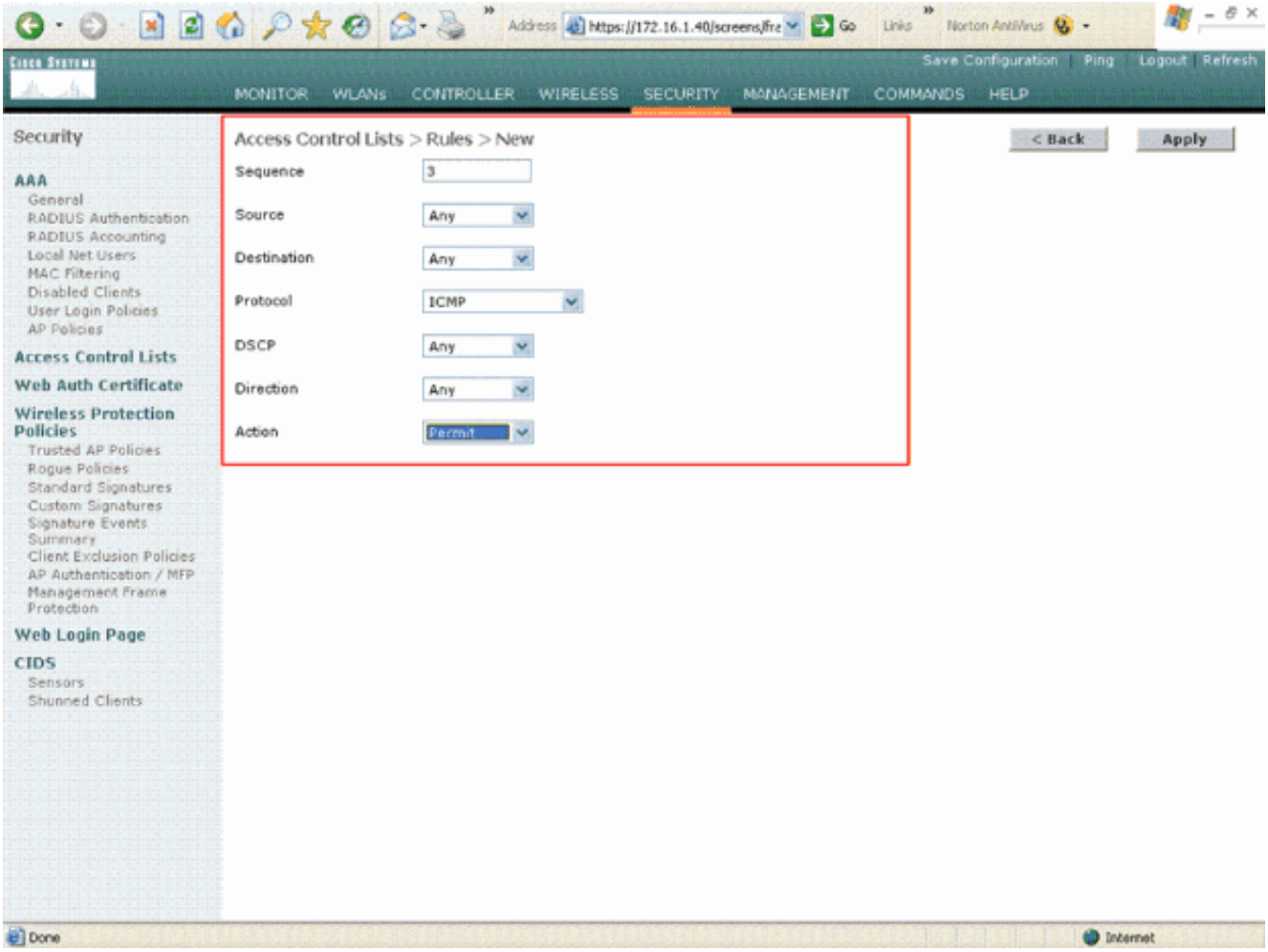
ます。 デフォルト値は [Deny] です。 [Apply] をクリックします。



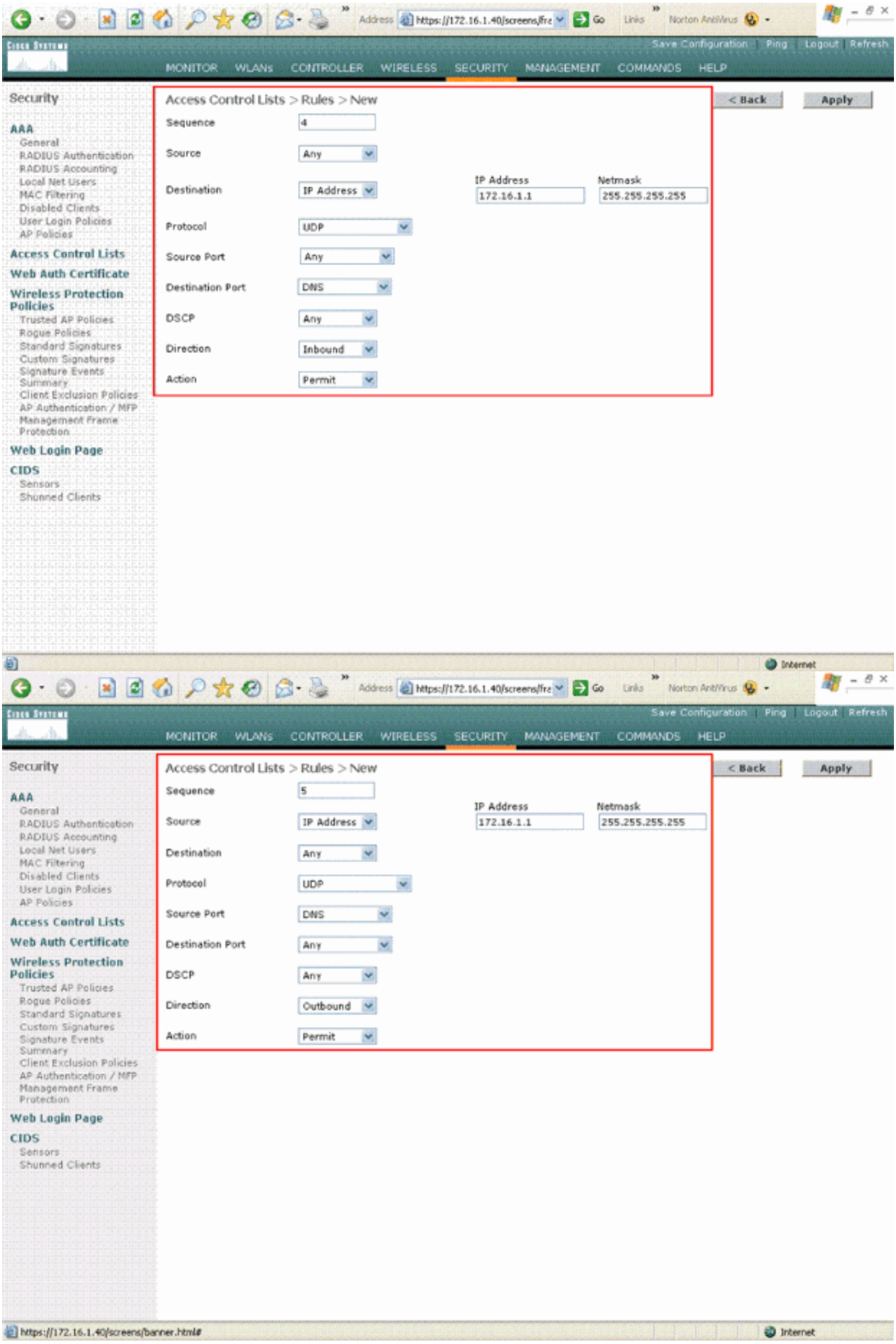
送信元と宛先のいずれかが **any** でない場合は、逆方向の inverse ステートメントを作成する必要があります。 次に例を示します。



2. 全デバイス間の ICMP パケットを許可するルールを定義するために、[Source] フィールドおよび [Destination] フィールドで **any** を選択します。 これがデフォルト値です。[Protocol] ドロップダウン フィールドから [ICMP] を選択します。 この例では、[Source] フィールドおよび [Destination] フィールドに **any** を使用するため、方向を指定する必要はありません。 デフォルト値の **any** にしておくことができます。 逆方向の inverse ステートメントも不要です。[Action] ドロップダウン メニューで、[Permit] を選択して、DHCP サーバからワイヤレス クライアントへの DHCP パケットがこの ACL によって許可されるようにします。 [Apply] をクリックします。

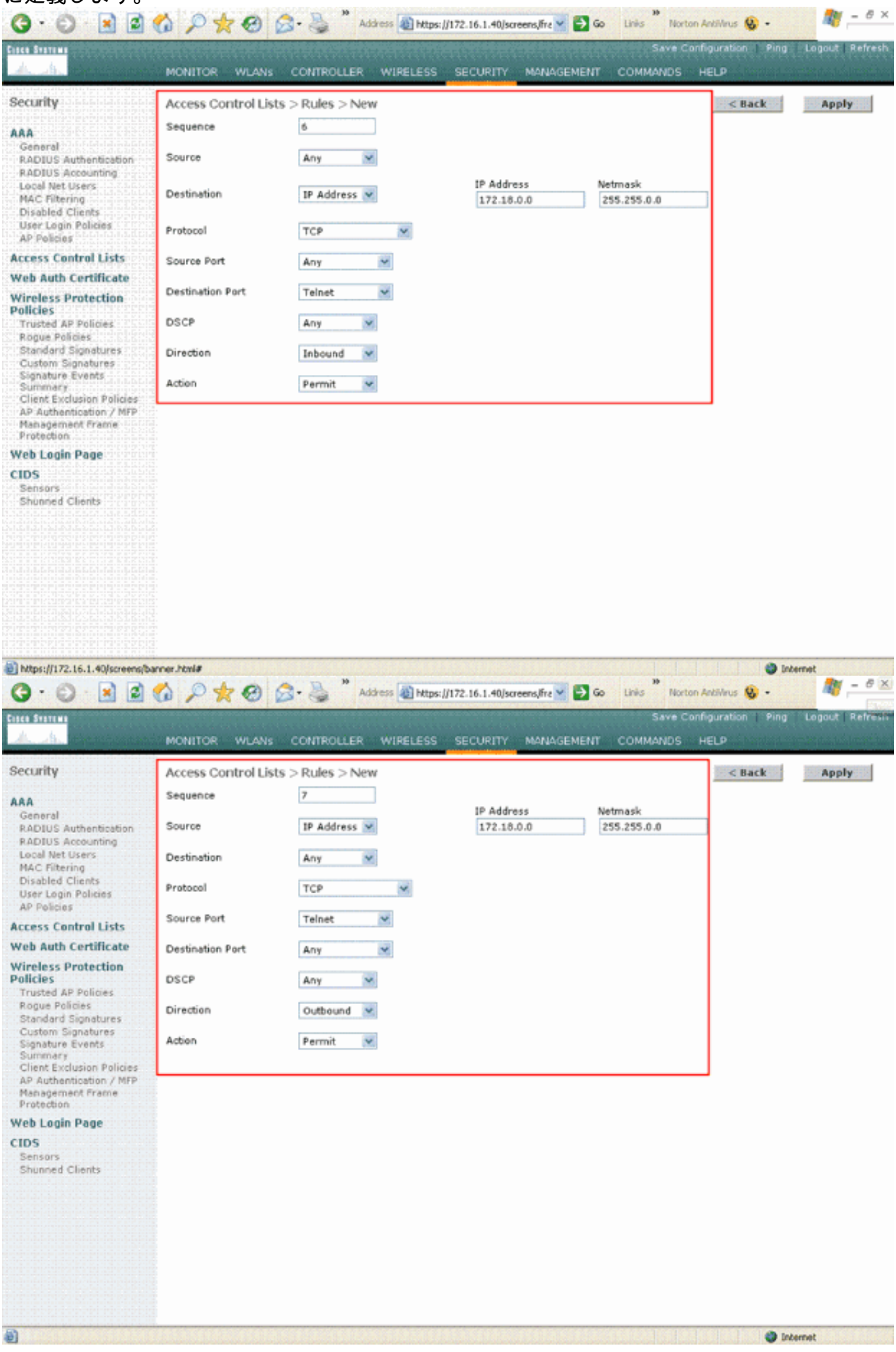


3. 同様に、すべてのワイヤレス クライアントに DNS サーバへのアクセスを許可するルールおよびワイヤレス クライアントのための Telnet サーバ アクセスを特定のサブネットに許可するルールを作成します。 次に例を示します。

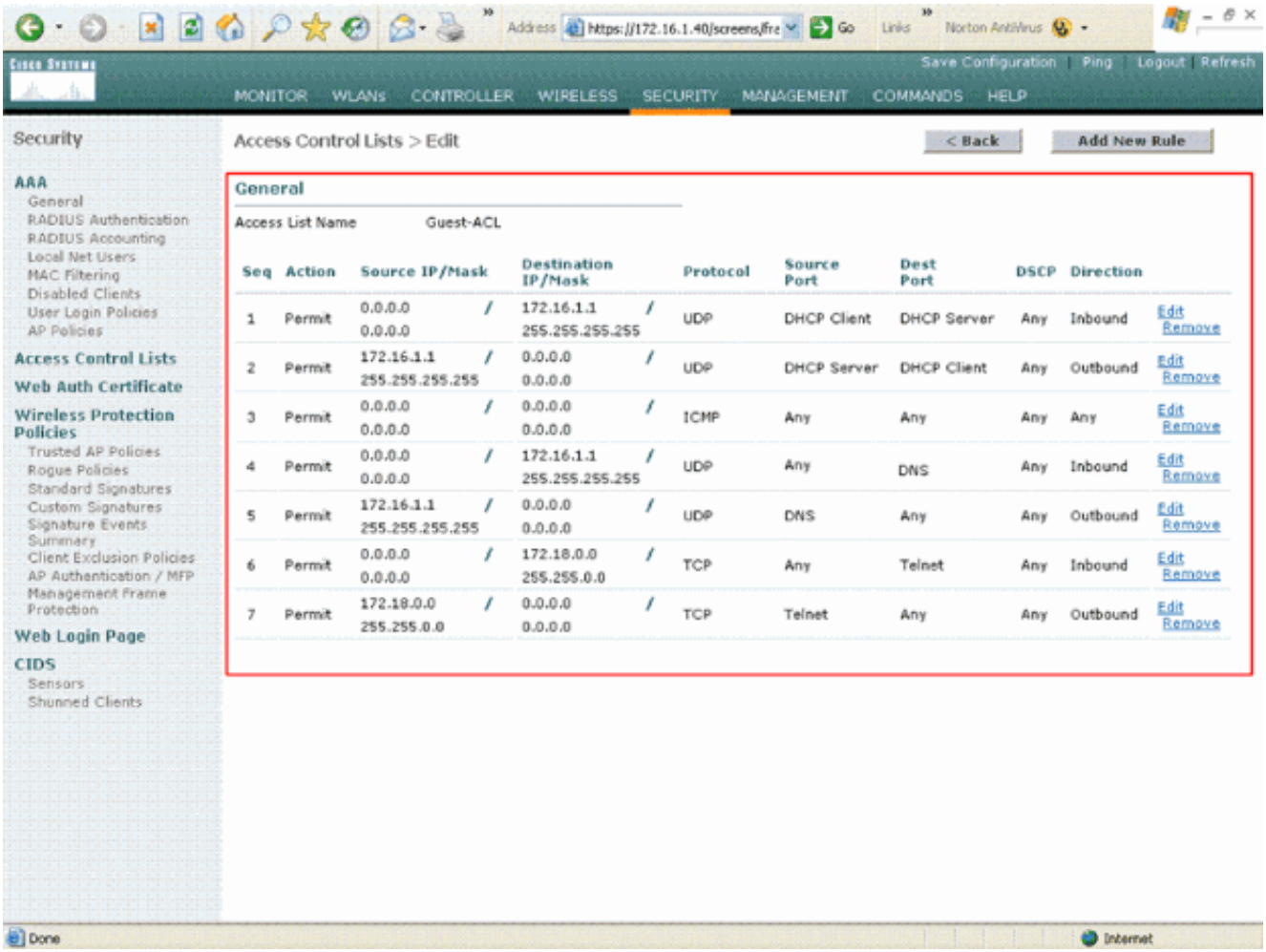


このルールは、ワイヤレス クライアントに、Telnet サービスへのアクセスを許可するため

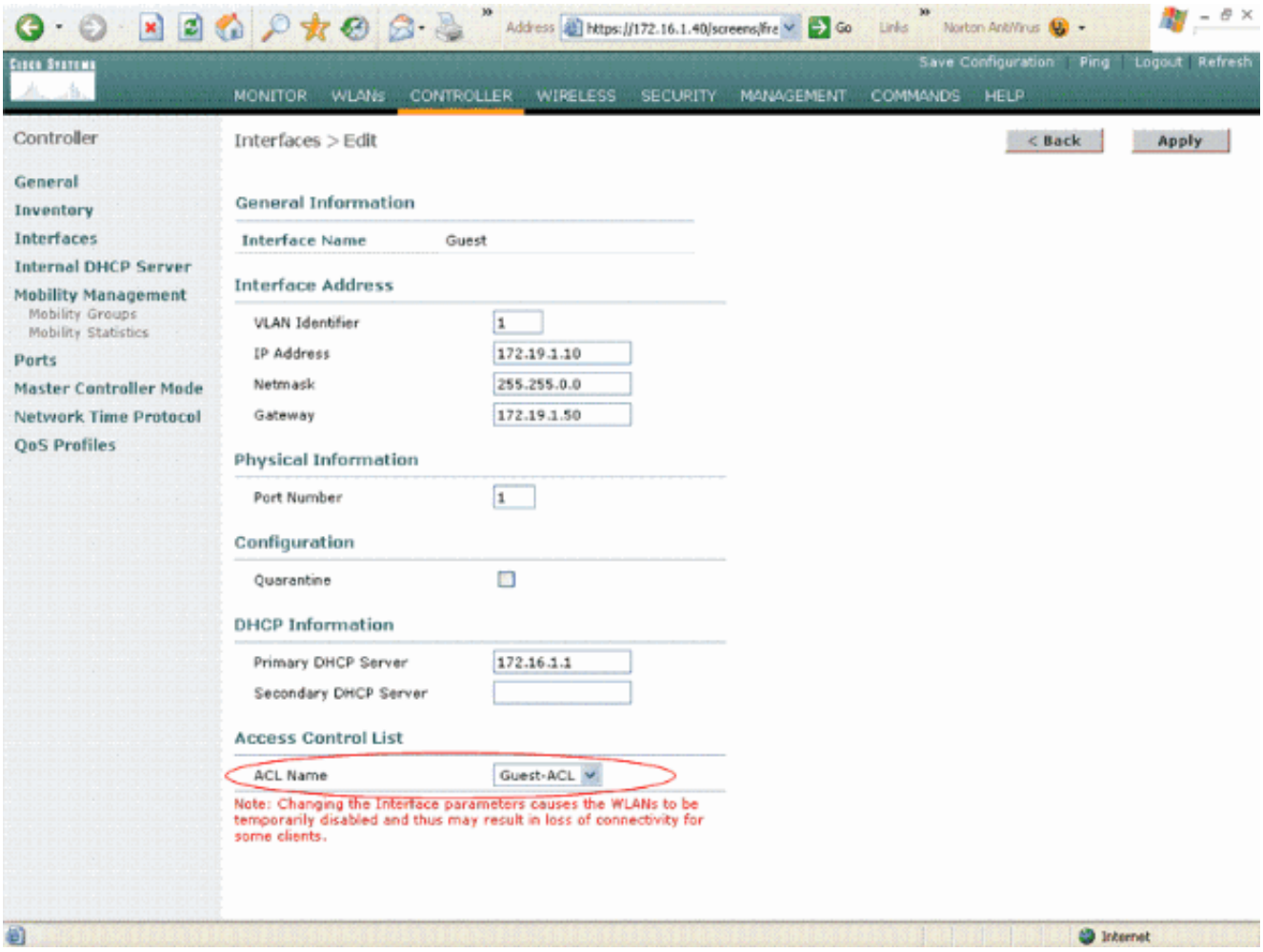
に定義します。


Address https://172.16.1.40/screens/fra
Go
Links
Norton AntiVirus
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 172.16.0.0
Netmask 255.255.0.0
Protocol TCP
Source Port Any
Destination Port Telnet
DSCP Any
Direction Inbound
Action Permit
https://172.16.1.40/screens/banner.html#
Internet
Address https://172.16.1.40/screens/fra
Go
Links
Norton AntiVirus
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 172.16.0.0
Netmask 255.255.0.0
Destination Any
Protocol TCP
Source Port Telnet
Destination Port Any
DSCP Any
Direction Outbound
Action Permit
Internet

[ACL > Edit] ページには、この ACL に定義されているすべてのルールの一覧が表示されます。



4. ACL が作成されたら、ダイナミック インターフェイスに適用する必要があります。 ACL を適用するには、[Controller] > [Interfaces] を選択し、ACL を適用するインターフェイスを編集します。
5. ダイナミック インターフェイスの [Interfaces > Edit] ページで、[Access Control Lists] ドロップダウン メニューから適切な ACL を選択します。 次に例を示します。



これを完了すると、このダイナミック インターフェイスを使用する WLAN 上で ACL によってトラフィックが許可および拒否されます (設定したルールに基づく) 。 インターフェイス ACL は、スタンドアロン モードの H-Reap AP には適用できず、接続モードだけに適用できます。

注: CLI を使用して WLC 上に ACL を作成する方法については、『CLI を使用したアクセス コントロール リストの設定』を参照してください。

注: このドキュメントでは、WLAN およびダイナミック インターフェイスは設定されていると想定しています。 WLC 上にダイナミック インターフェイスを作成する方法については、『無線 LAN コントローラでの VLAN の設定例』を参照してください。

CPU ACL の設定

これまで、WLC 上の ACL には、管理インターフェイス宛ておよび AP マネージャ インターフェイス宛ての LWAPP/CAPWAP データ トラフィック、LWAPP/CAPWAP 制御トラフィック、モビリティ トラフィックをフィルタリングするオプションがありませんでした。 この問題に対処し、LWAPP およびモビリティ トラフィックをフィルタリングするために、WLC ファームウェア リリース 4.0 で CPU ACL が導入されました。

CPU ACL の設定には、2 つの手順が含まれています。

1. CPU ACL のためのルールを設定します。
2. CPU ACL を WLC に適用します。

CPU ACL のルールは、他の ACL と同様に設定する必要があります。 CPU ACL の詳細については、『Wireless LAN Controller (WLC) の保護』の「CPU ACL」を参照してください。

確認

正しく設定したことを確認するために、ワイヤレス クライアントを使用して ACL 設定をテストすることを推奨します。 正しく動作しない場合は、ACL Web ページで ACL を確認し、ACL に対する変更がコントローラのインターフェイスに適用されたことを確認してください。

設定は、次の **show** コマンドを使用して確認することもできます。

- **show acl summary**：コントローラ上に設定されている ACL を表示するには、**show acl summary** コマンドを使用します。次に例を示します。

```
(Cisco Controller) >show acl summary

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

- **show acl detailed ACL_Name**：設定されている ACL の詳細情報が表示されます。次に例を示します。

```
(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**：CPU 上に設定されている ACL を表示するには、**show acl cpu** コマンドを使用します。次に例を示します。

```
(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
```

トラブルシューティング

コントローラ ソフトウェア リリース 4.2.61.0 以降では、ACL カウンタを設定できます。 ACL カウンタによって、コントローラを介して送信されたパケットに適用された ACL を判別しやすくなることがあります。 この機能は、システムをトラブルシューティングするときに有用です。

ACL カウンタは、次のコントローラで使用可能です。

- 4400 シリーズ
- Cisco WiSM
- Catalyst 3750G Integrated Wireless LAN Controller スイッチ

この機能を有効に設定するには、次の手順を実行します。

1. [Security] > [Access Control Lists] > [Access Control Lists] を選択して、[Access Control Lists] ページを開きます。このページでは、このコントローラに設定されているすべての ACL が表示されます。
2. パケットがコントローラ上で設定されている ACL のいずれかに一致しているかどうかを確認するには、[Enable Counters] チェックボックスをオンにして、[Apply] をクリックします。 それ以外の場合は、このチェック ボックスをオフにします。 これがデフォルト値です。
3. ACL のカウンタをクリアするには、その ACL の青いドロップダウンの矢印の上にカーソルを置いて、[Clear Counters] を選択します。

関連情報

- アクセス コントロール リストの設定と適用
- 無線 LAN コントローラでの VLAN の設定例
- Wireless LAN Controller (WLC) への Lightweight AP (LAP) の登録
- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.0
- ワイヤレス/モビリティに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems