ワイヤレスLANコントローラでのACLの設定例

内容

概要

このドキュメントでは、ワイヤレスLANコントローラ(WLAN)でアクセスコントロールリスト(ACL)を設定して、WLAN経由でトラフィックをフィルタリングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- WLCとLightweightアクセスポイント(LAP)の基本動作の設定方法
- 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いています。

- 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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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、ACLは管理インターフェイス上でバイパスされるため、WLC宛てのトラフィックに影響を与えることはできません。**Management Via Wireless**オプションを使用してコントローラの管理をワイヤレスクライアントに対して妨げることができるだけです。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。詳細については、「CPU ACLの設定」セクションを参照してください。

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。

- sourceand destinationが **any**の場合、このACLが適用される方向は**any**になります。
- sourceordestinationのいずれかがanyでない場合は、フィルタの方向を指定し、逆方向のinverse文を作成する必要があります。
- WLCのインバウンドとアウトバウンドの概念は直感的ではありません。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でACLを設定する際の考慮事項

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パケットの内部にあるものを選択するため、IP-in-IPパケットを拒否または許可します。
- コントローラACLは、WLCの仮想IPアドレスをブロックできないため、ワイヤレスクライアントのDHCPパケットをブロックできません。
- コントローラACLは、ワイヤレスクライアントを宛先とする有線ネットワークから受信した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、ワイヤレスクライアントから開始され、同じコントローラ上の有線ネットワークまたはその他のワイヤレスクライアントを宛先とするマルチキャストトラフィックに対して処理されます。
- 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。リターントラフィック用

にACLに穴を開け忘れると、問題が発生します。
- 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:ACLをインターフェイスまたはWLANに適用すると、ワイヤレススループットが低下し、パケットが失われる可能性があります。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。

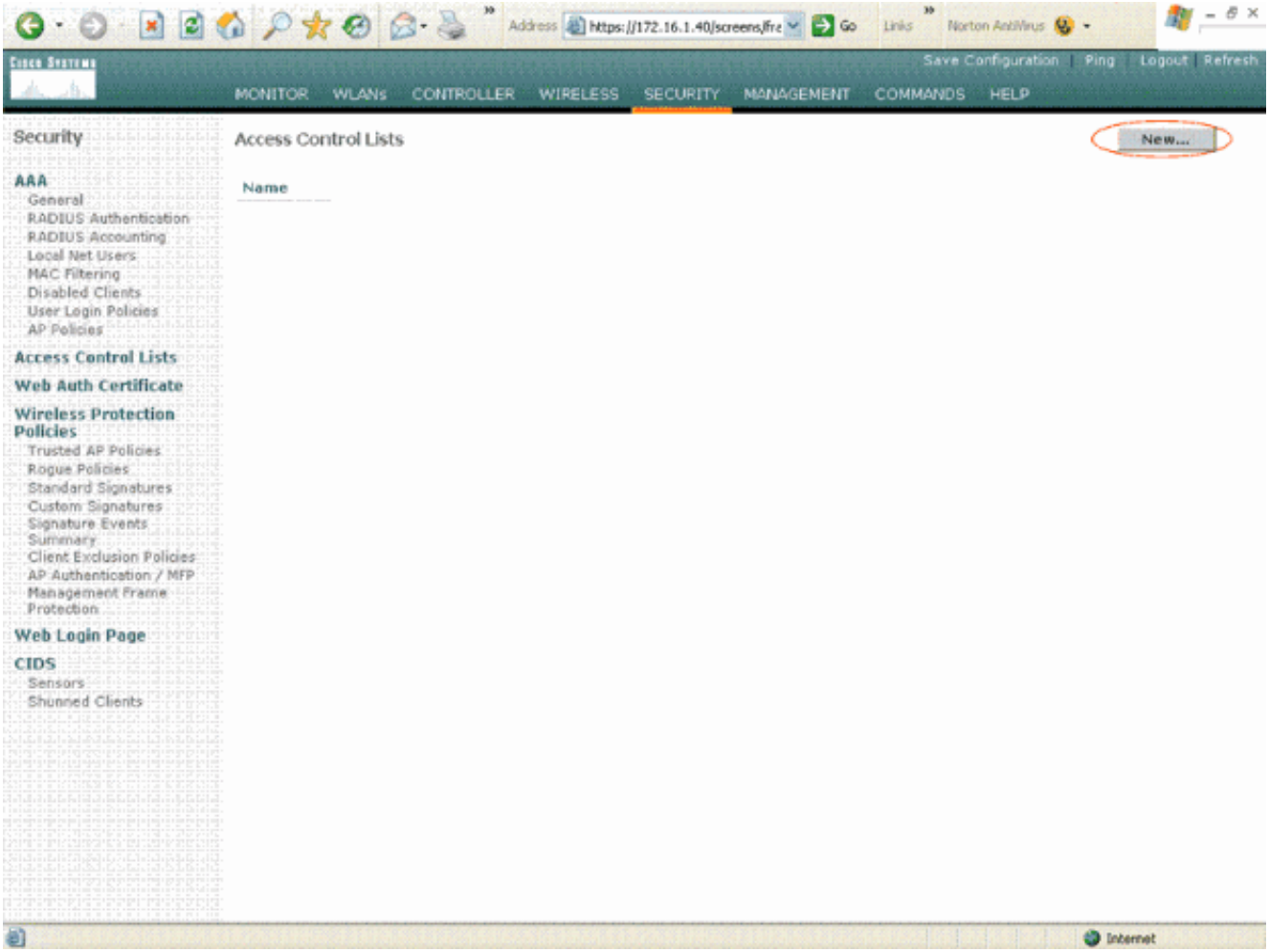
WLC 上の ACL の設定

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

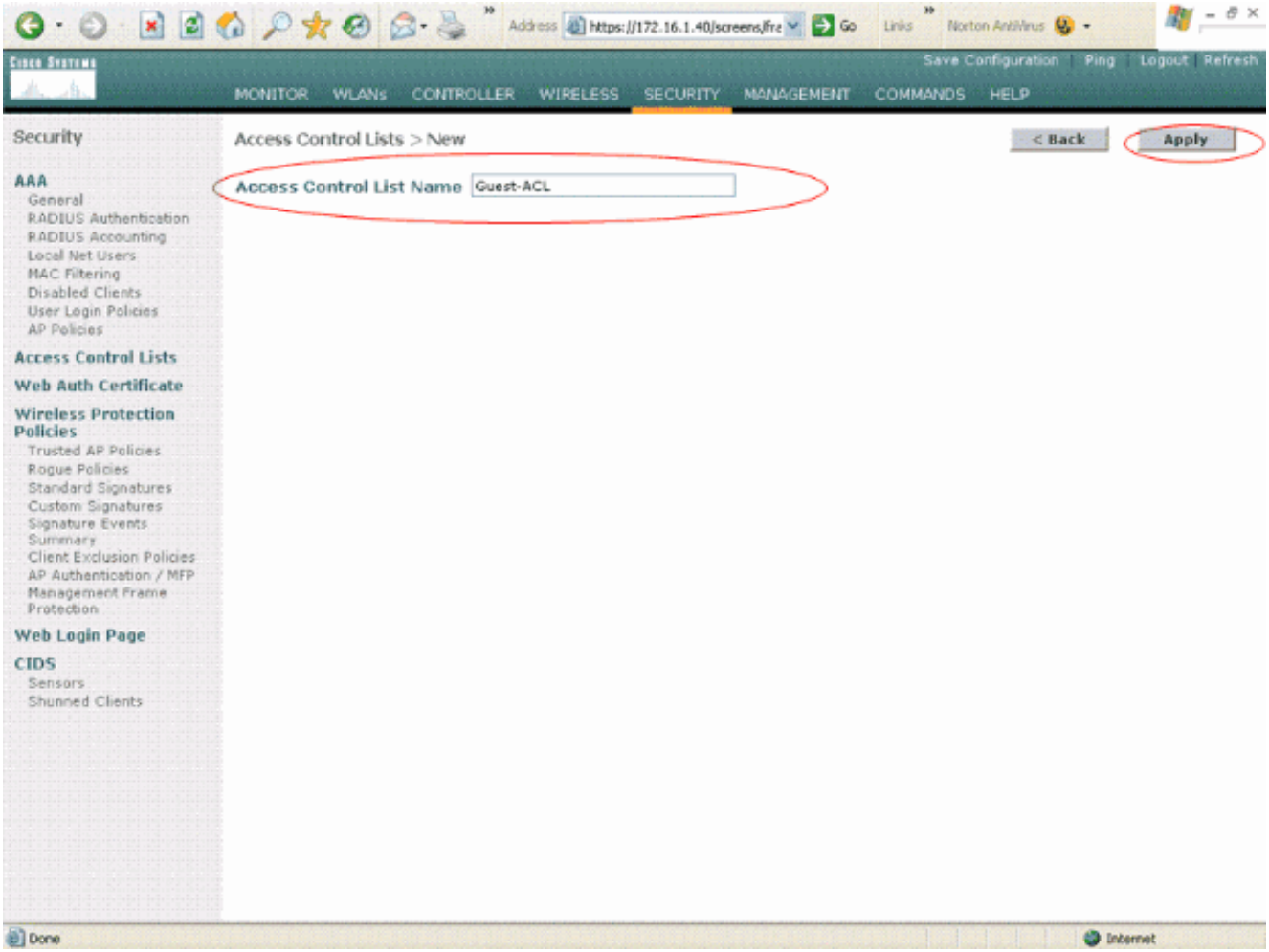
このワイヤレス クライアントに対する他のすべてのサービスはブロックされる必要があります。WLC GUIを使用してACLを作成するには、次の手順を実行します。

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。



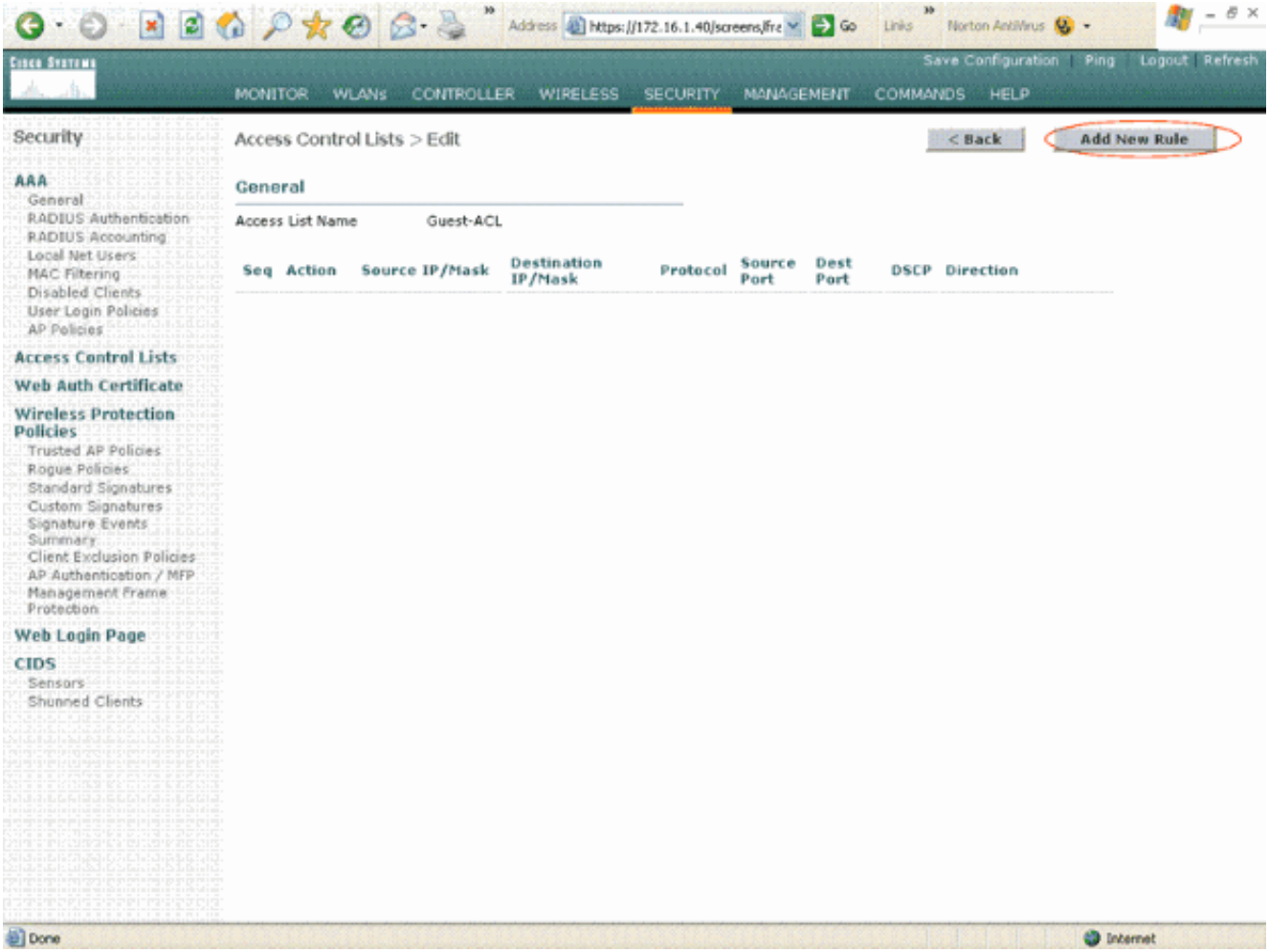
アクセス コントロール リスト

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を作成したら、[Edit] をクリックしてACLのルールを作成します。



ACLの名前を入力します。

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。



新しいACLルールの追加

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

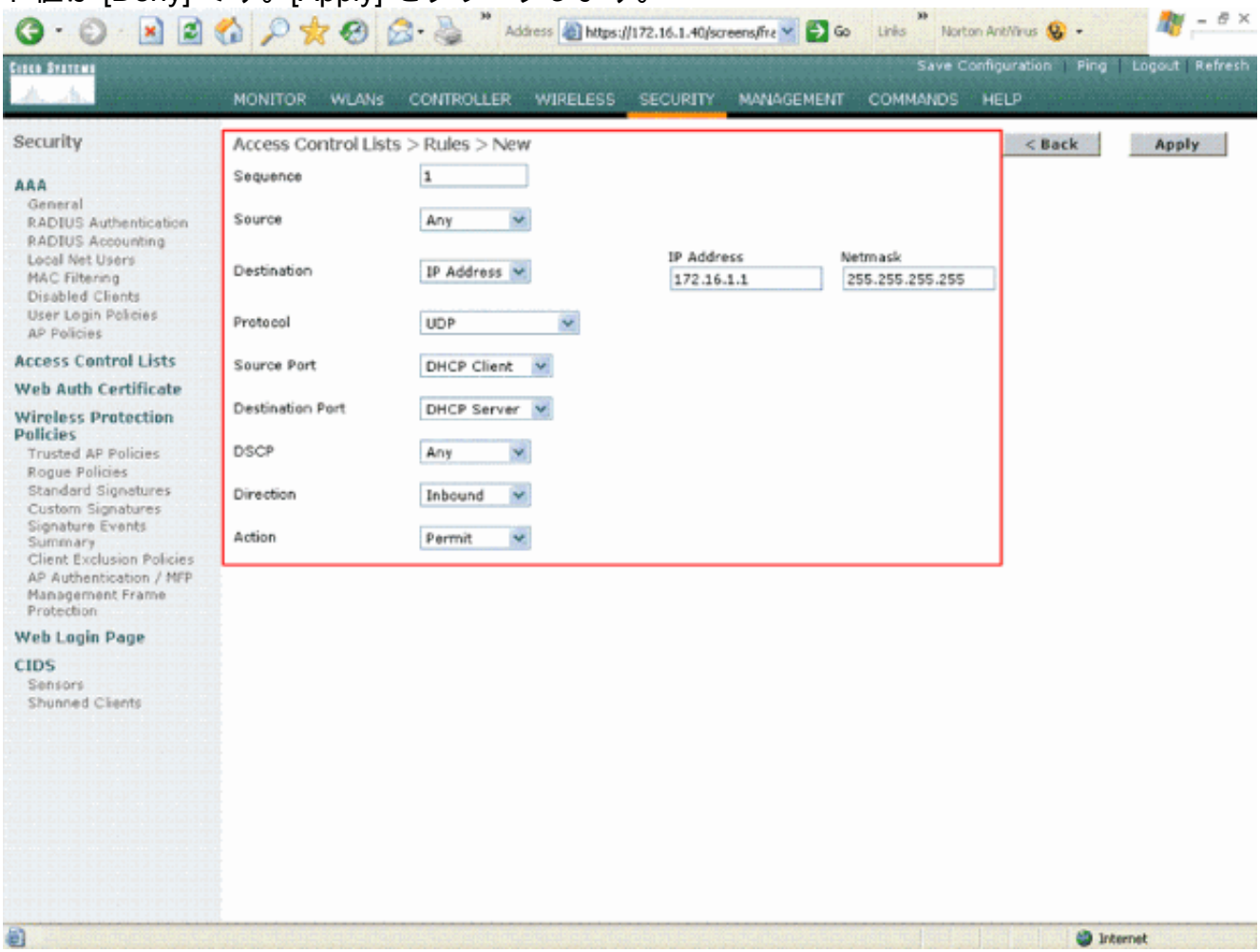
ゲスト ユーザ サービスを可能にするルールの設定

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。

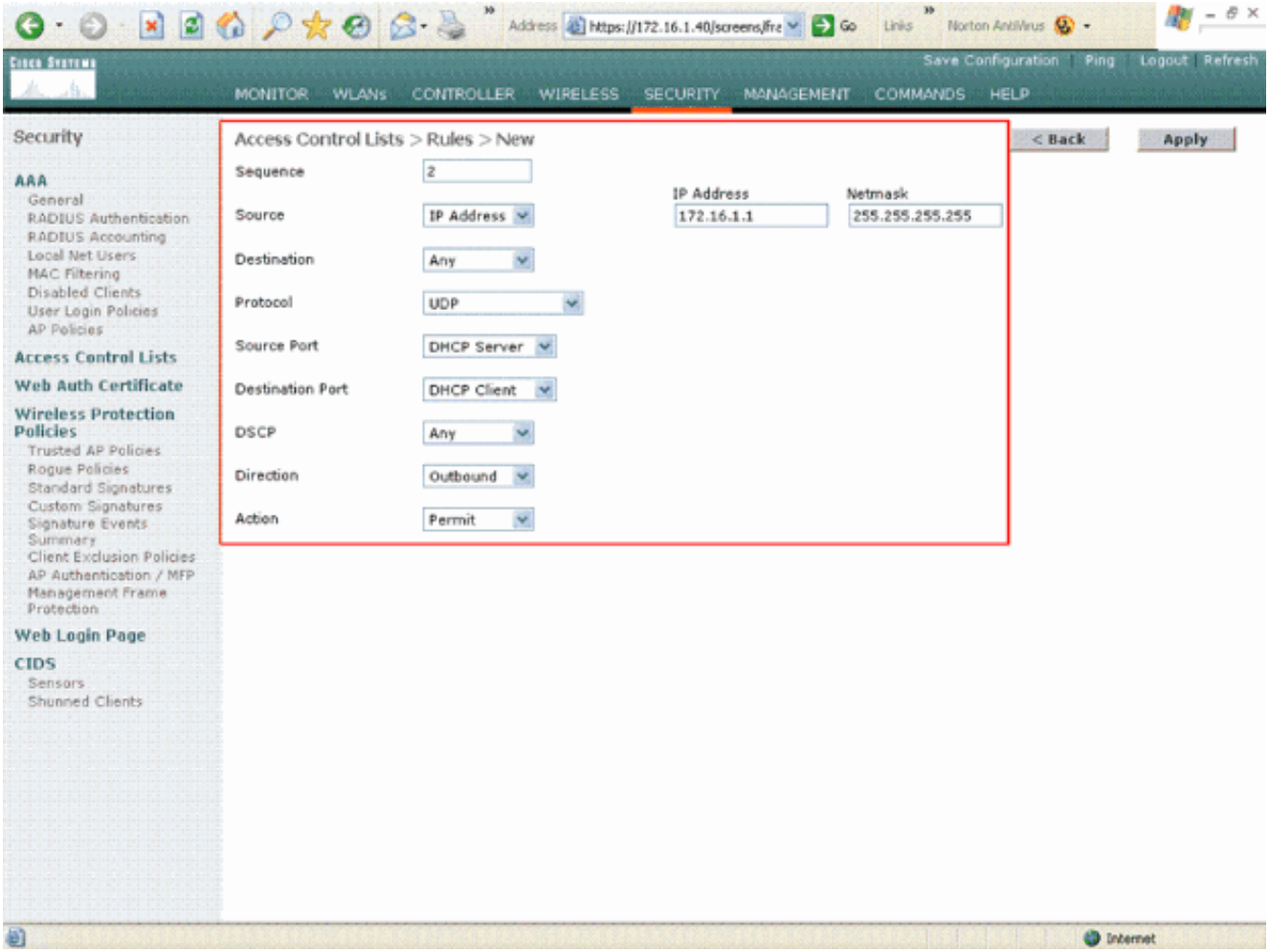
- ワイヤレス クライアントと DHCP サーバの間の DHCP
- ネットワーク内の全デバイス間の ICMP
- ワイヤレス クライアントと DNS サーバの間の DNS
- 特定のサブネットへの Telnet

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、さらに[Source Port]と[Destination Port]の2つのパラメータが表示されます。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。

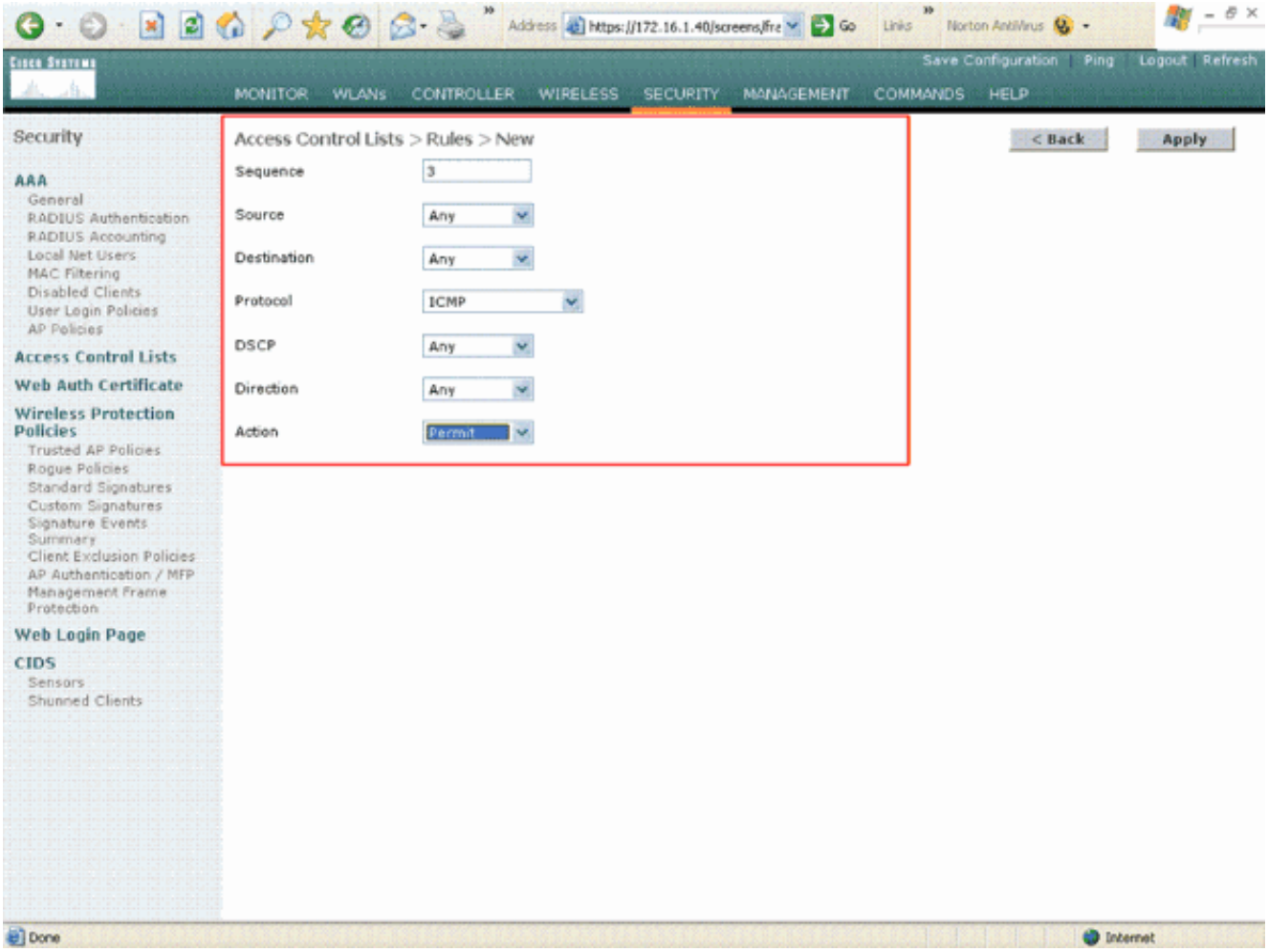


[Permit]を選択してACLでDHCPパケットを許可する 送信元と宛先のいずれかが **any でない場合は、逆方向の inverse ステートメントを作成する必要があります。**次に例を示します。



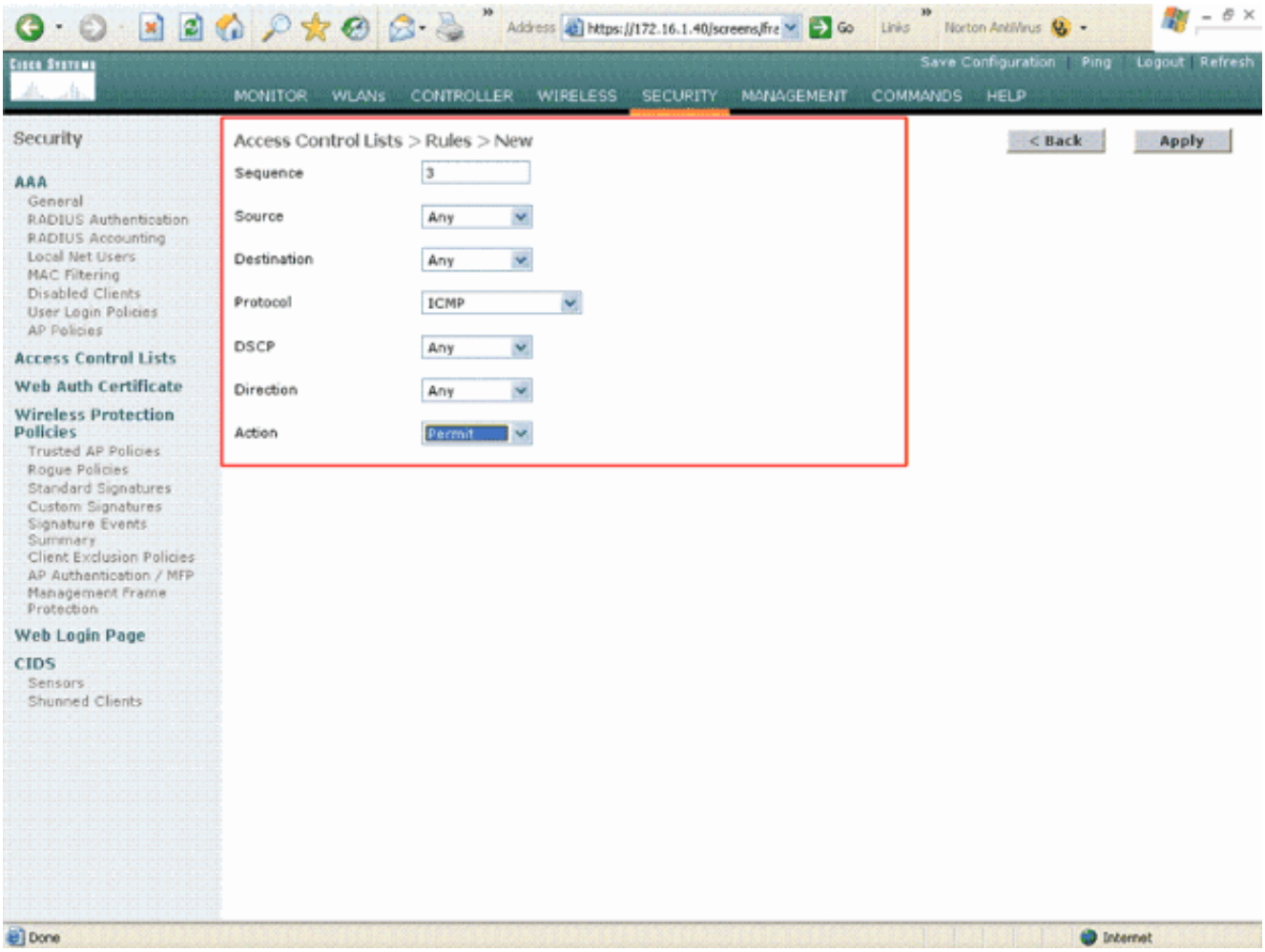
[Source or Destination]を[Any]に設定

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。

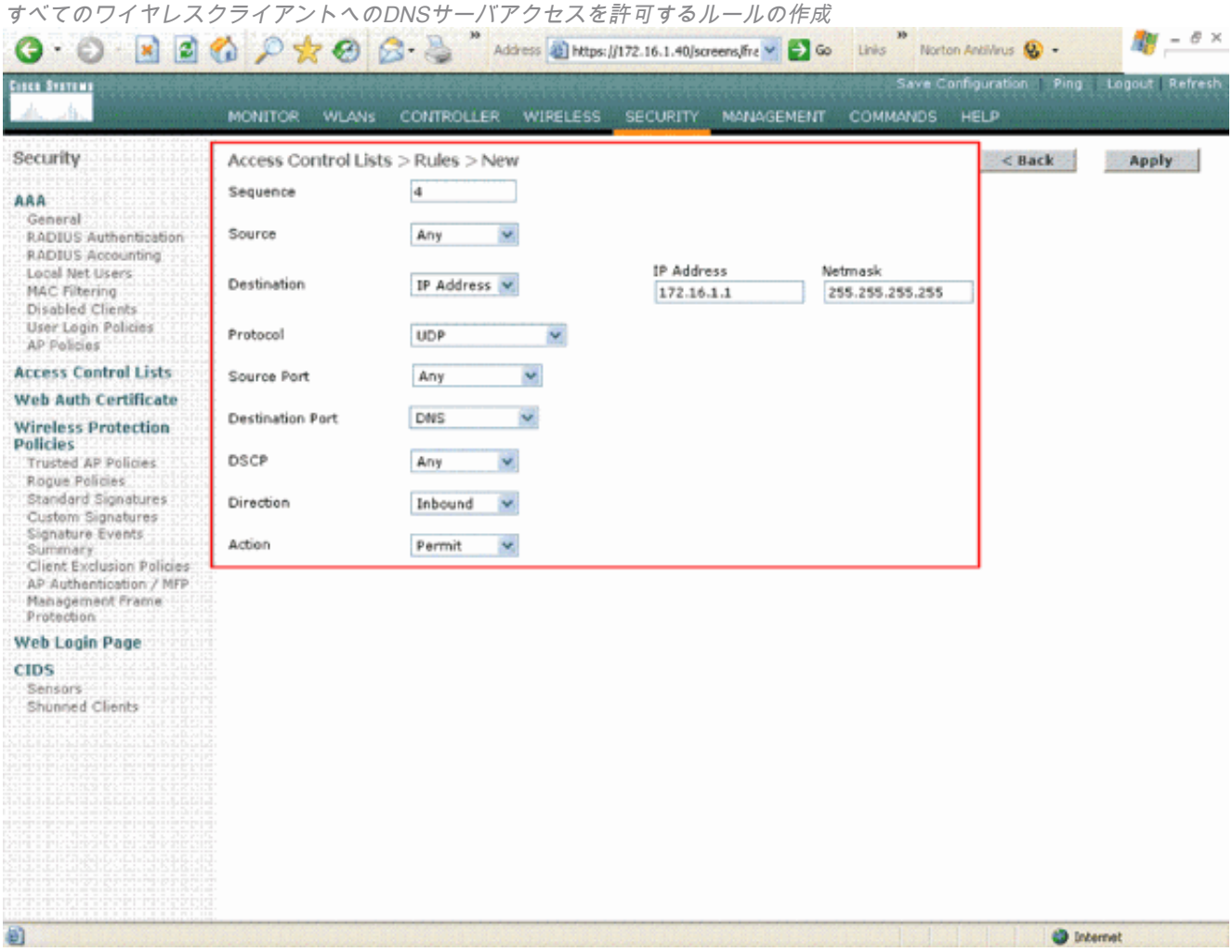


ACLでDHCPサーバからワイヤレスクライアントへのDHCPパケットを許可する許可

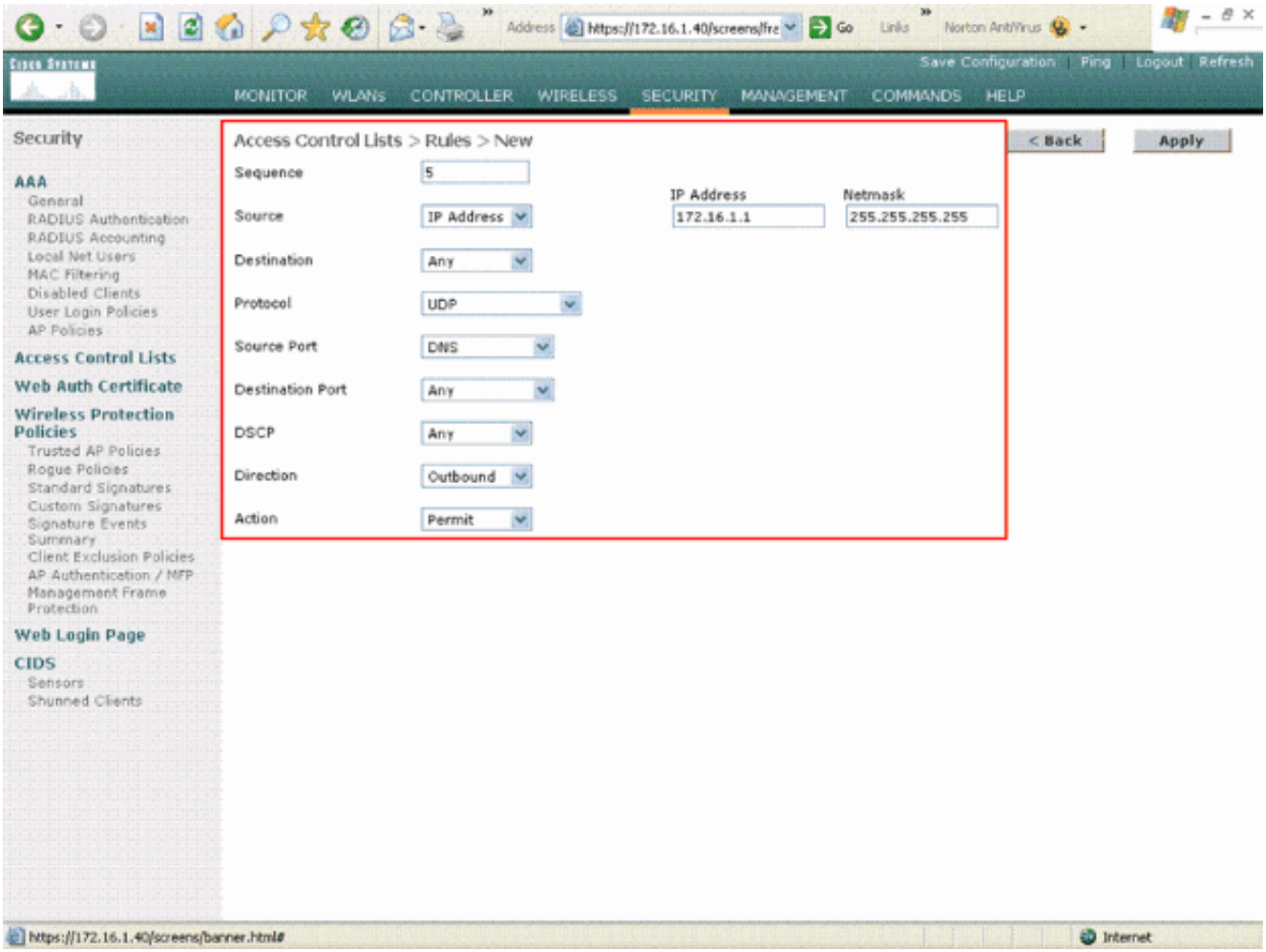
3. 同様に、すべてのワイヤレス クライアントに DNS サーバへのアクセスを許可するルールおよびワイヤレス クライアントのための Telnet サーバ アクセスを特定のサブネットに許可するルールを作成します。次に例を示します。



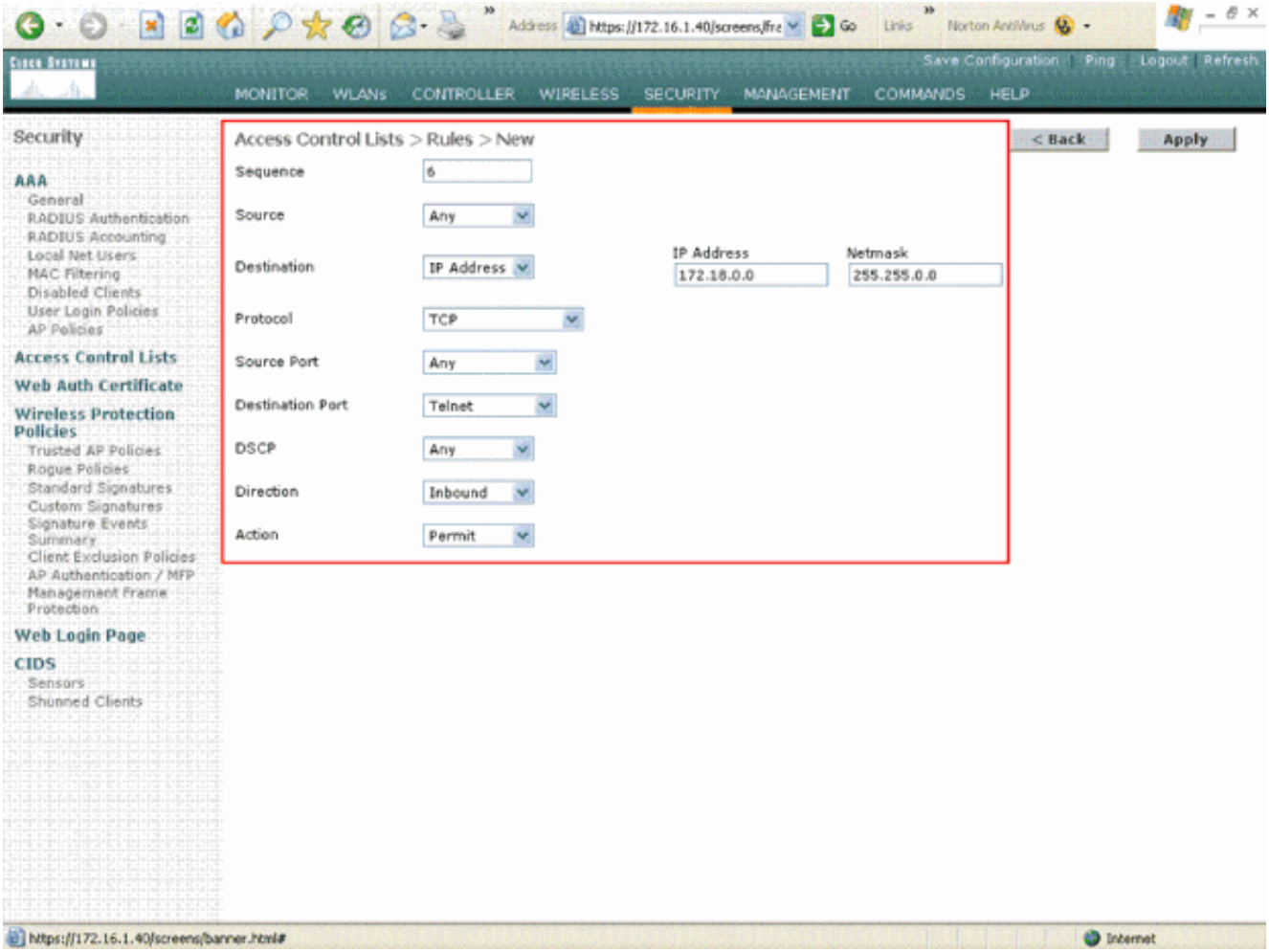
すべてのワイヤレスクライアントへのDNSサーバアクセスを許可するルールの作成



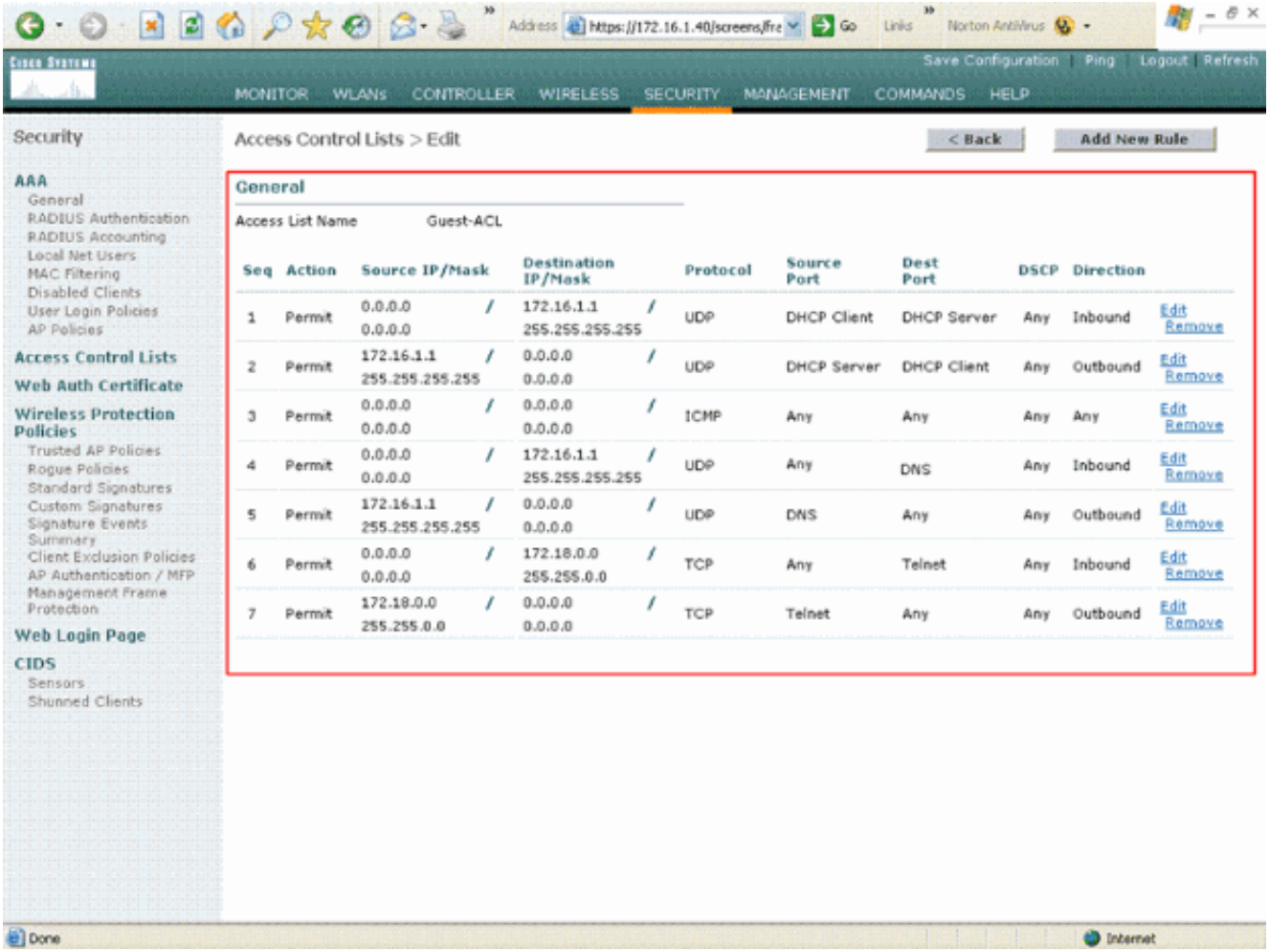
サブネットへのワイヤレスクライアントのTelnetサーバアクセスを許可するルールの作成 このルールは、ワイヤレス クライアントに、Telnet サービスへのアクセスを許可するために定義します。



Telnetサービスへのワイヤレスクライアントのアクセスを許可する

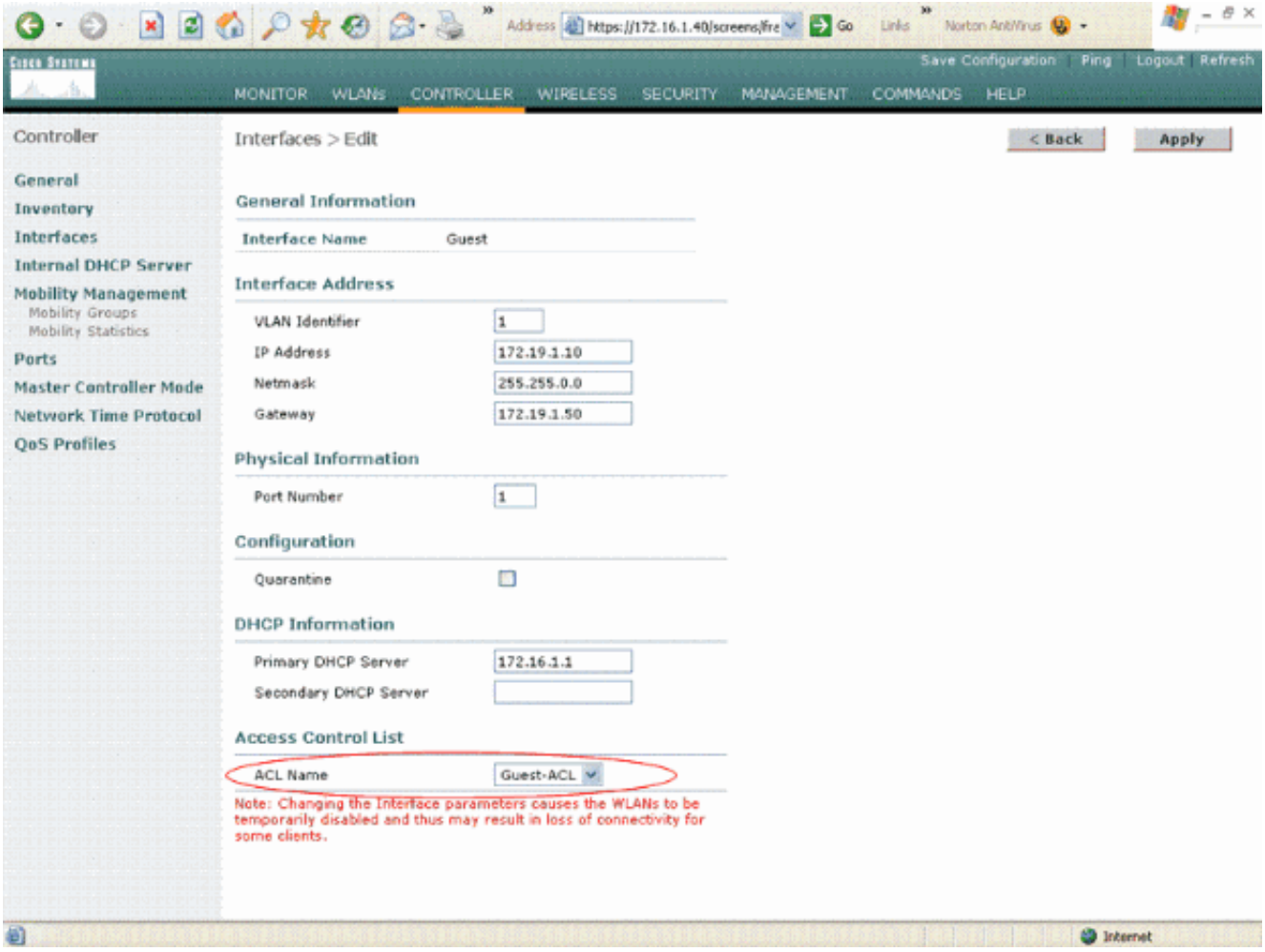


Telnetサービスへのワイヤレスクライアントアクセスの別の例 [ACL > Edit] ページには、この ACL に定義されているすべてのルールの一覧が表示されます。



[Edit]ページには、ACLに定義されているすべてのルールがリストされます

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。



[Access Control List]メニューから適切なACLを選択します

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**：このドキュメントでは、WLANとダイナミックインターフェイスが設定されていることを前提としています。WLCで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、『ワイヤレスLANコントローラでのVLANの設定』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。

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の変更がコントローラインターフェイスに適用されたことを確認します。

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。**以下が一例です。

```
(Cisco Controller) >show acl summary

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

- **show acl detailedACL_Name**：設定されたACLの詳細情報を表示します。以下が一例です。

```
(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。**以下が一例です。

```
(Cisco Controller) >show acl cpu

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

トラブルシュート

コントローラソフトウェアリリース4.2.x以降では、ACLカウンタを設定できます。ACLカウンタは、コントローラを介して送信されたパケットにどのACLが適用されたかを判断するのに役立ちます。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に設定されたACLのいずれかにヒットす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

- Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 6.0
- ワイヤレスLANコントローラでのVLANの設定
- WLC に接続できない Lightweight AP のトラブルシューティング
- シスコテクニカルサポートおよびダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。