在無線LAN控制器上設定ACL範例

目錄

簡介

本檔案介紹如何在無線LAN控制器(WLAN)上設定存取控制清單(ACL)，以過濾通過WLAN的流量。

必要條件

需求

思科建議您瞭解以下主題：

- 如何設定WLC和輕量型存取點(LAP)以達成基本操作
- 輕量型存取點通訊協定(LWAPP)和無線安全方法的基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行韌體4.0的Cisco 2000系列WLC
- Cisco 1000系列LAP
- 運行韌體2.6的Cisco 802.11a/b/g無線客戶端介面卡
- Cisco Aironet案頭公用程式(ADU)版本2.6

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

WLC上的ACL

WLC上的ACL旨在限制或允許無線使用者端使用其WLAN上的服務。

在WLC韌體版本4.0之前，ACL會在管理介面上略過，因此您無法影響目的地為WLC的流量，而只能使用**Management Via Wireless** 選項防止無線使用者端管理控制器。因此，ACL只能應用於動態介面。在WLC韌體版本4.0中，有一些CPU ACL可以過濾目的地為管理介面的流量。有關詳細資訊，請參閱配置CPU ACL部分。

您可以定義最多64個ACL，每個最多包含64個規則（或過濾器）。每個規則都有影響其操作的引數。當資料包匹配規則的所有引數時，該規則的操作集將應用於資料包。您可以通過GUI或CLI配置ACL。

在WLC上設定ACL之前，需要瞭解以下一些規則：

- 如果sourceanddestination為any，則此ACL的應用方向可以為**any**。
- 如果sourceordestination不是any，則必須指定過濾器的方向，並且必須建立相反方向的反向語句。
- WLC的入站和出站概念是不直觀的。它從WLC面向無線客戶端的角度出發，而不是從客戶端的角度出發。因此，傳入方向是指從無線使用者端傳入WLC的封包，傳出方向是指從WLC傳出至無線使用者端的封包。
- ACL的結尾有隱含的deny。

在WLC中配置ACL時的注意事項

WLC中的ALC與路由器中的不同。在WLC中設定ACL時，請記住以下幾點：

- 最常見的錯誤是在您打算拒絕或允許IP資料包時選擇IP。由於您選擇IP封包中的內容，因此您可以拒絕或允許IP內IP封包。
- 控制器ACL無法封鎖WLC虛擬IP位址，因此也無法封鎖無線使用者端的DHCP封包。
- 控制器 ACL 無法封鎖從有線網路接收，以無線用戶端為目的地的多點傳送流量。控制器 ACL 用於處理從無線用戶端發起，以有線網路或相同控制器上的其他無線用戶端為目的地的多點傳送流量。
- 與路由器不同，ACL應用於介面時可以控制兩個方向的流量，但不會執行狀態防火牆。如果您忘記在ACL中開啟回傳流量的洞孔，就會出現問題。
- 控制器ACL僅阻止IP資料包。您不能阻止非IP的第2層ACL或第3層資料包。
- 控制器ACL不會像路由器那樣使用反向遮罩。這裡的255表示與IP位址八位元完全相符。
- 控制器上的ACL是在軟體中完成的，會影響轉發效能。

  註：如果將ACL應用於介面或WLAN，無線吞吐量會降低，並可能導致資料包丟失。為了提高吞吐量，請從介面或WLAN中刪除ACL，然後將ACL移動到相鄰的有線裝置。

在WLC上設定ACL

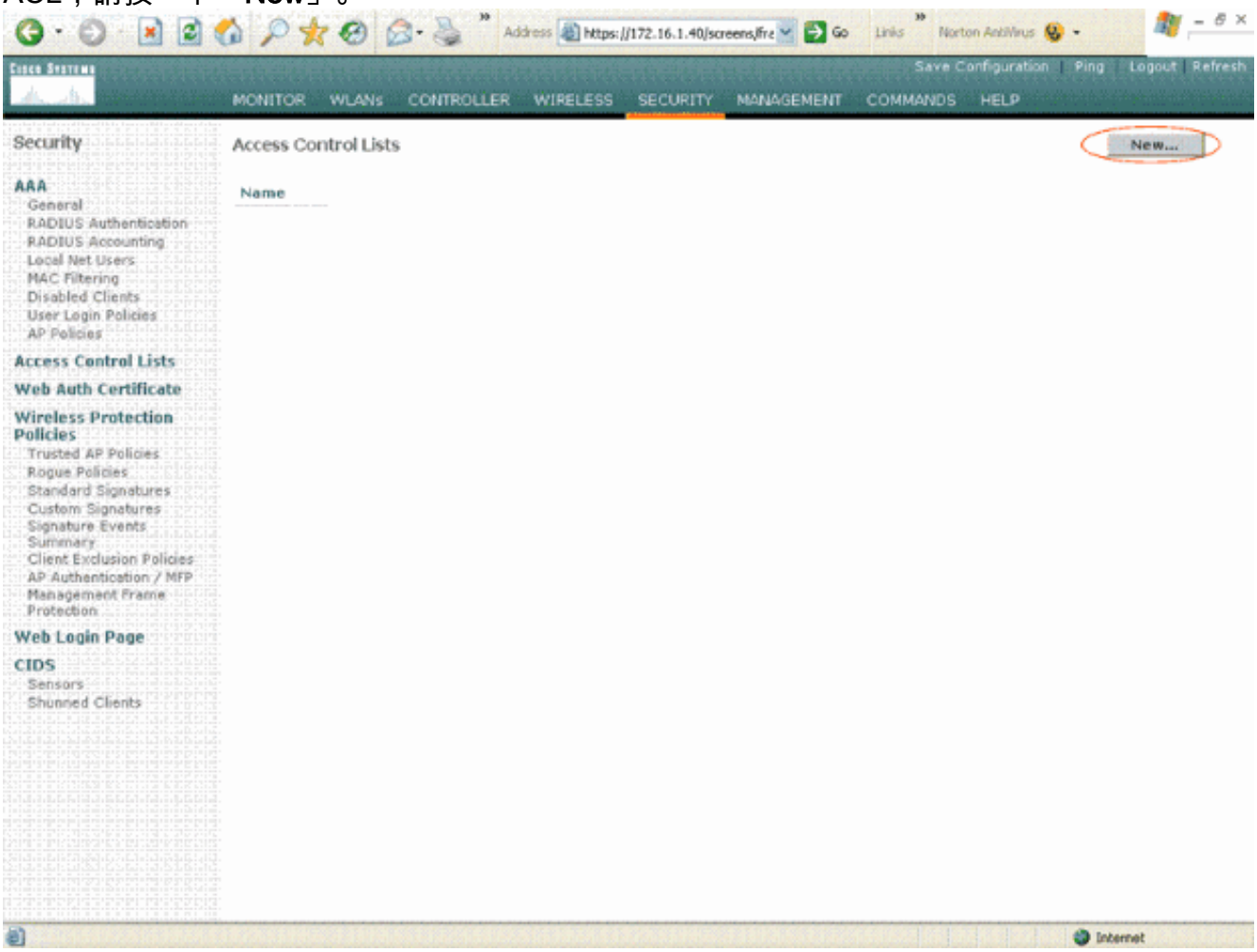
本節介紹如何在WLC上設定ACL。目標是配置允許訪客客戶端訪問以下服務的ACL:

- 無線客戶端和DHCP伺服器之間的動態主機配置協定(DHCP)

- 網路中所有裝置之間的網際網路控制訊息通訊協定(ICMP)
- 無線客戶端和DNS伺服器之間的域名系統(DNS)
- Telnet至特定子網

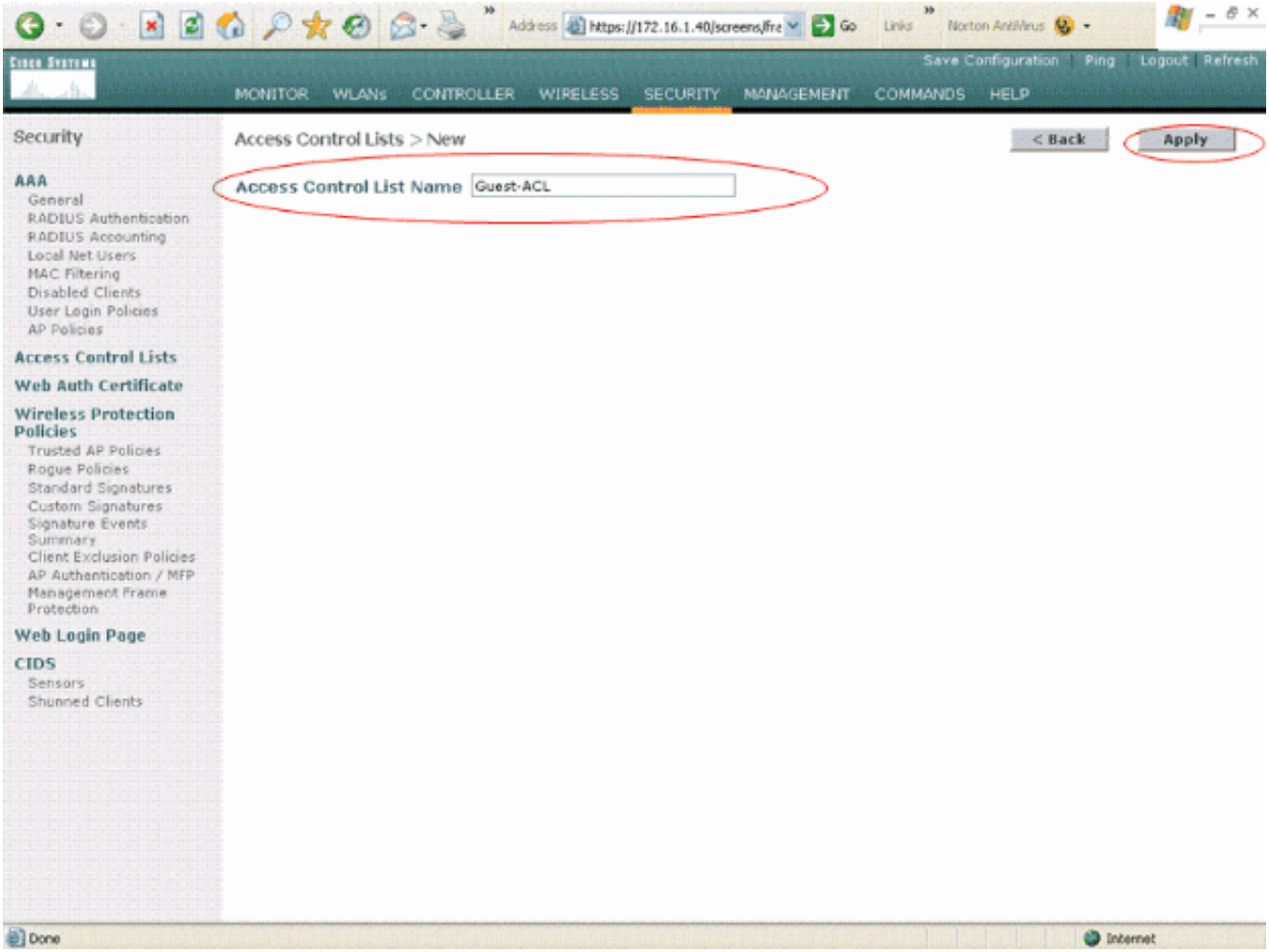
必須阻止無線客戶端的所有其他服務。完成以下步驟，以便使用WLC GUI建立ACL:

1. 前往WLC GUI，然後選擇**Security > Access Control Lists**。系統將顯示Access Control Lists頁面。此頁面列出在WLC上設定的ACL。此功能也允許您編輯或刪除任何ACL。若要建立新的ACL，請按一下「**New**」。



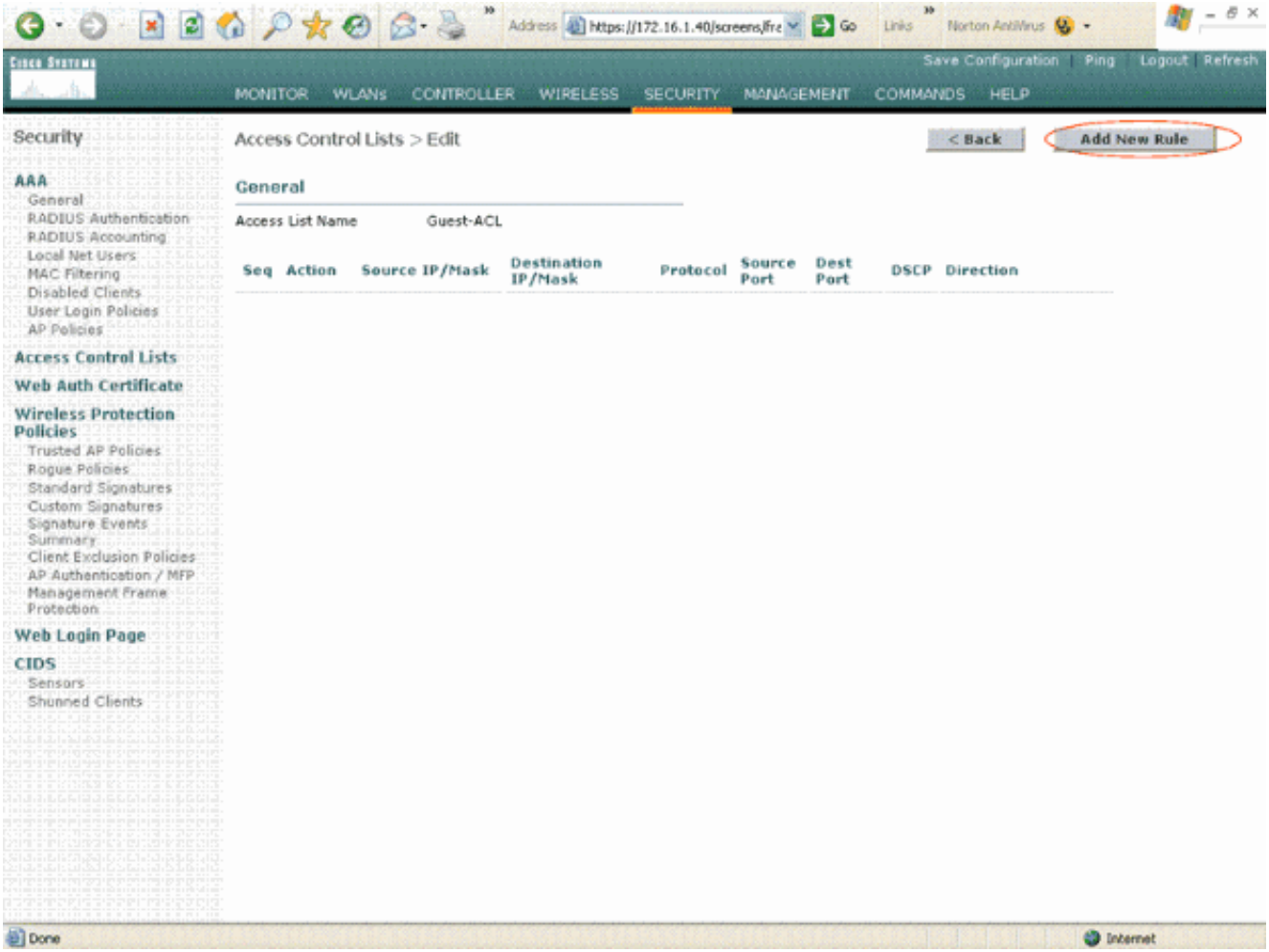
存取控制清單

2. 輸入ACL的名稱，然後按一下**Apply**。最多可輸入32個字母數字字元。在本範例中，ACL的名稱是**Guest-ACL**。建立ACL後，按一下**Edit**為ACL建立規則。



輸入ACL的名稱

3. 出現「訪問控制清單」(Access Control Lists)>「編輯」(Edit)頁面時，單擊**「新增新規則」(Add New Rule)**。系統將顯示Access Control Lists > Rules > New頁面。



新增新的ACL規則

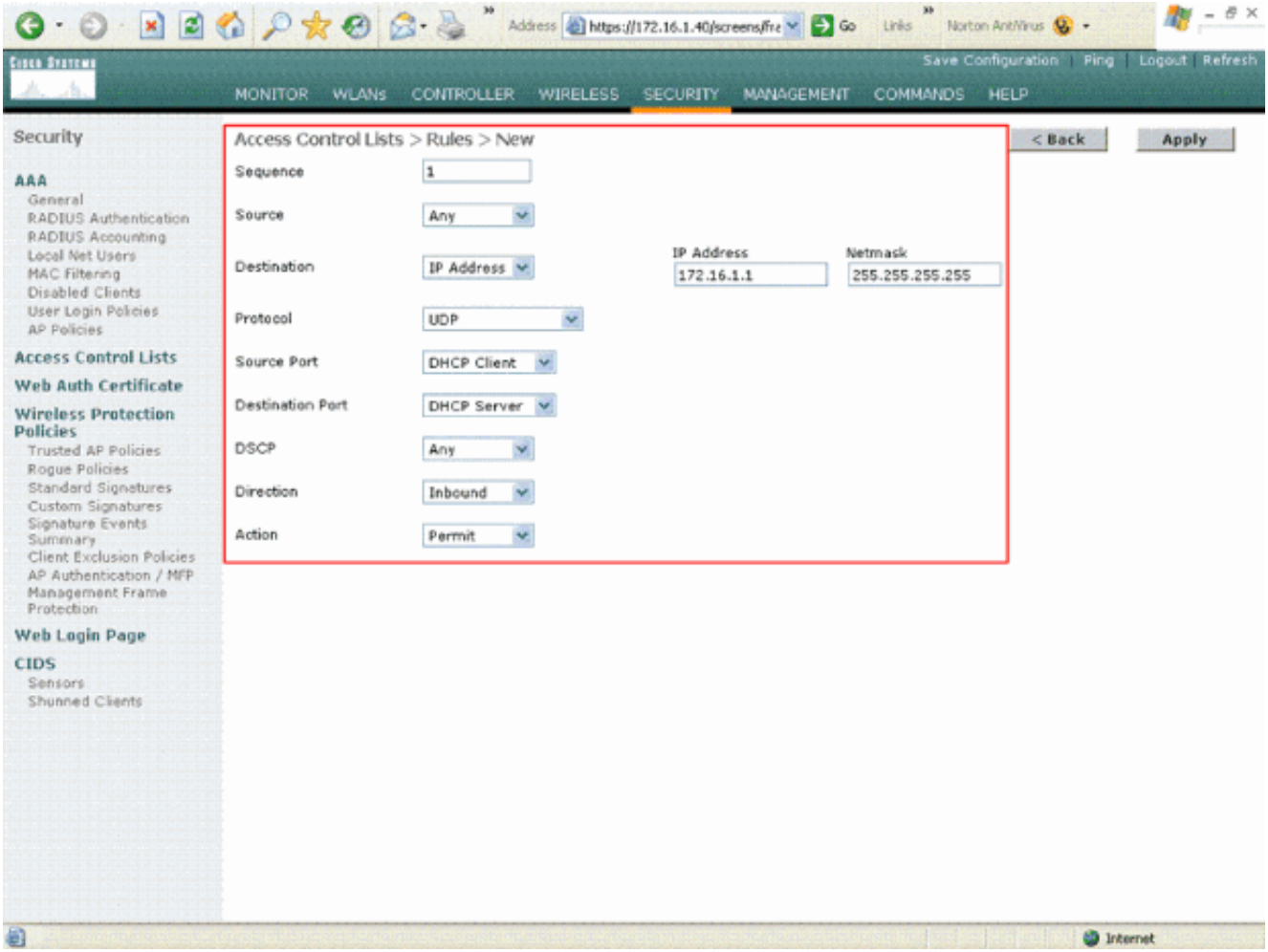
4. 配置允許訪客使用者使用這些服務的規則：無線客戶端和DHCP伺服器之間的DHCP網路中所有裝置之間的ICMP無線客戶端和DNS伺服器之間的DNSTelnet至特定子網

配置允許訪客使用者服務的規則

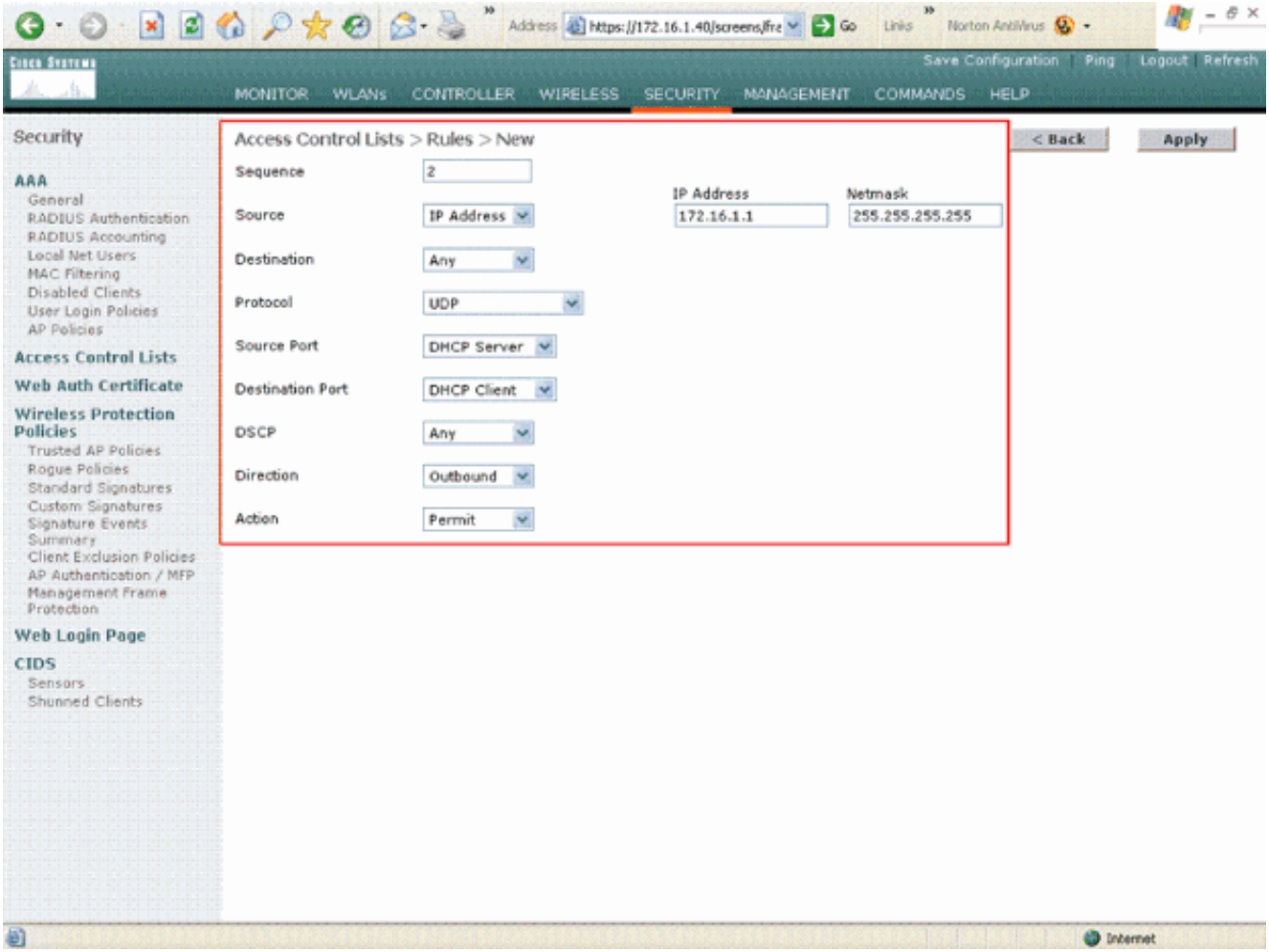
本節顯示如何配置這些服務的規則的示例：

- 無線客戶端和DHCP伺服器之間的DHCP
- 網路中所有裝置之間的ICMP
- 無線客戶端和DNS伺服器之間的DNS
- Telnet至特定子網

1. 要定義DHCP服務的規則，請選擇源IP範圍和目標IP範圍。此示例使用**any**作為源，這意味著允許任何無線客戶端訪問DHCP伺服器。在本示例中，伺服器172.16.1.1充當DHCP和DNS伺服器。因此，目的IP地址為172.16.1.1/255.255.255.255（帶主機掩碼）。因為DHCP是基於UDP的協定，所以從Protocol下拉欄位中選擇**UDP**。如果在上一步中選擇了TCP或UDP，則會顯示兩個附加引數：源埠和目的埠。指定源埠和目標埠詳細資訊。對於此規則，源埠是**DHCP Client**，目標埠是**DHCP Server**。選擇要應用ACL的方向。由於此規則是從客戶端到伺服器，因此本示例使用**入站**。在Action下拉框中，選擇**Permit**以使此ACL允許從無線客戶端到DHCP伺服器的DHCP資料包。預設值為Deny。按一下「**Apply**」。

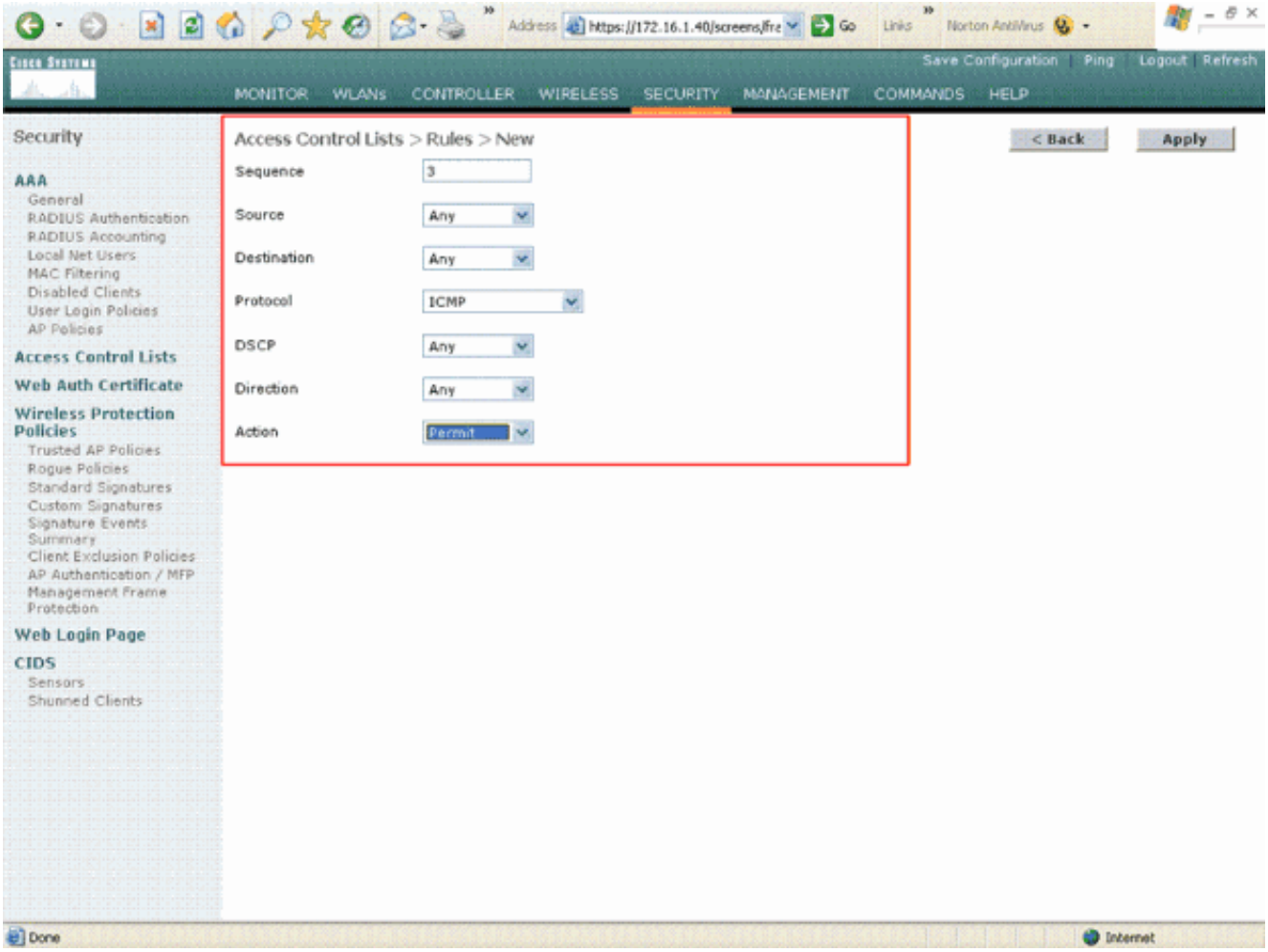


選擇Permit以使ACL允許DHCP資料包 如果源或目標不是**any**，則必須建立相反方向的反向語句。以下提供範例。



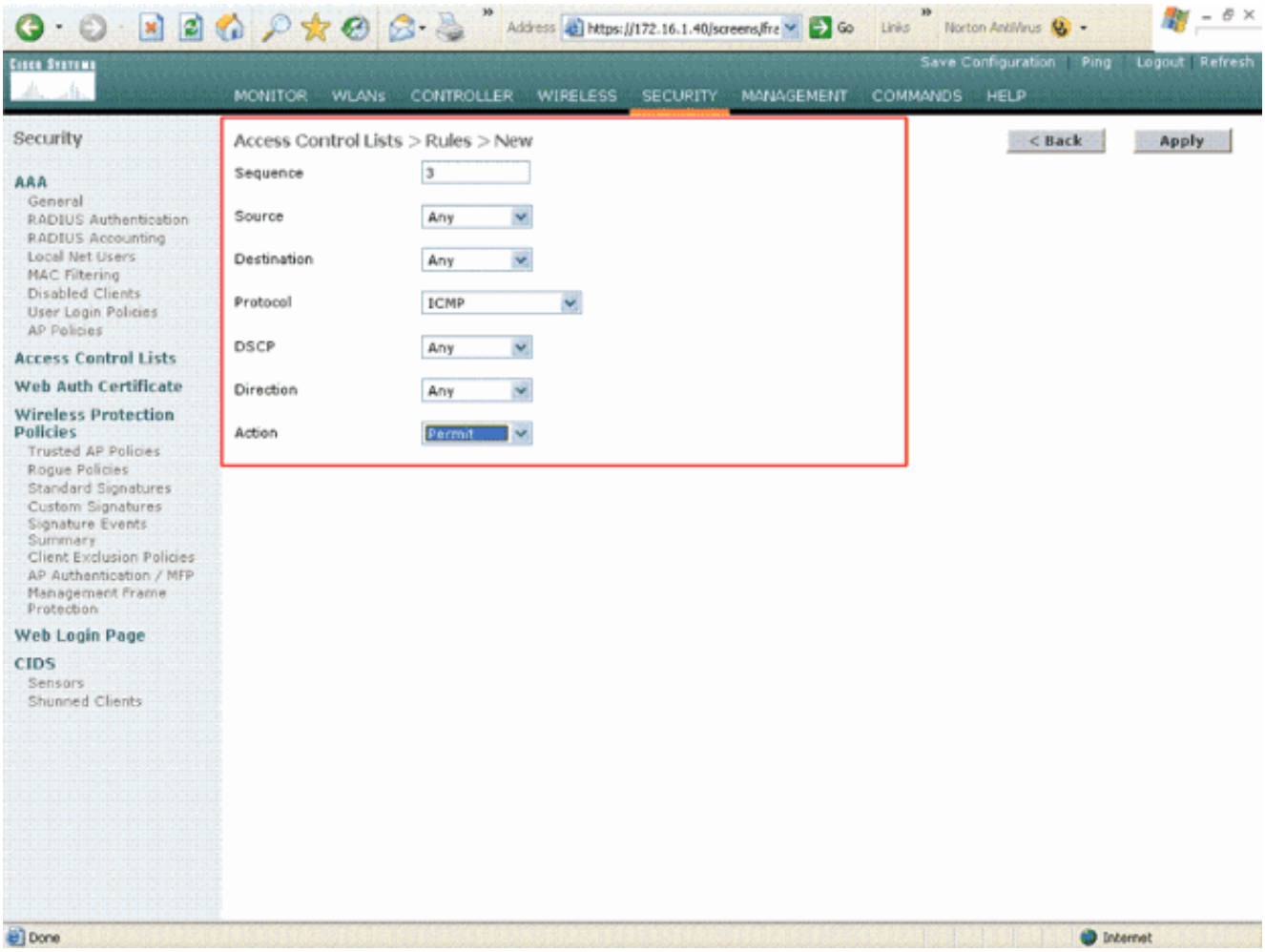
源或目標設定為Any

2. 要定義允許所有裝置之間的ICMP資料包的規則，請為**Source**和Destination欄位選擇any。這是預設值。從Protocol下拉欄位中選擇**ICMP**。由於此示例將**any**用於「源」和「目標」欄位，因此您不必指定方向。可以保留其預設值**any**。此外，不需要反向的反向語句。在Action下拉選單中，選擇**Permit**以使此ACL允許從DHCP伺服器到無線客戶端的DHCP資料包。按一下「Apply」。

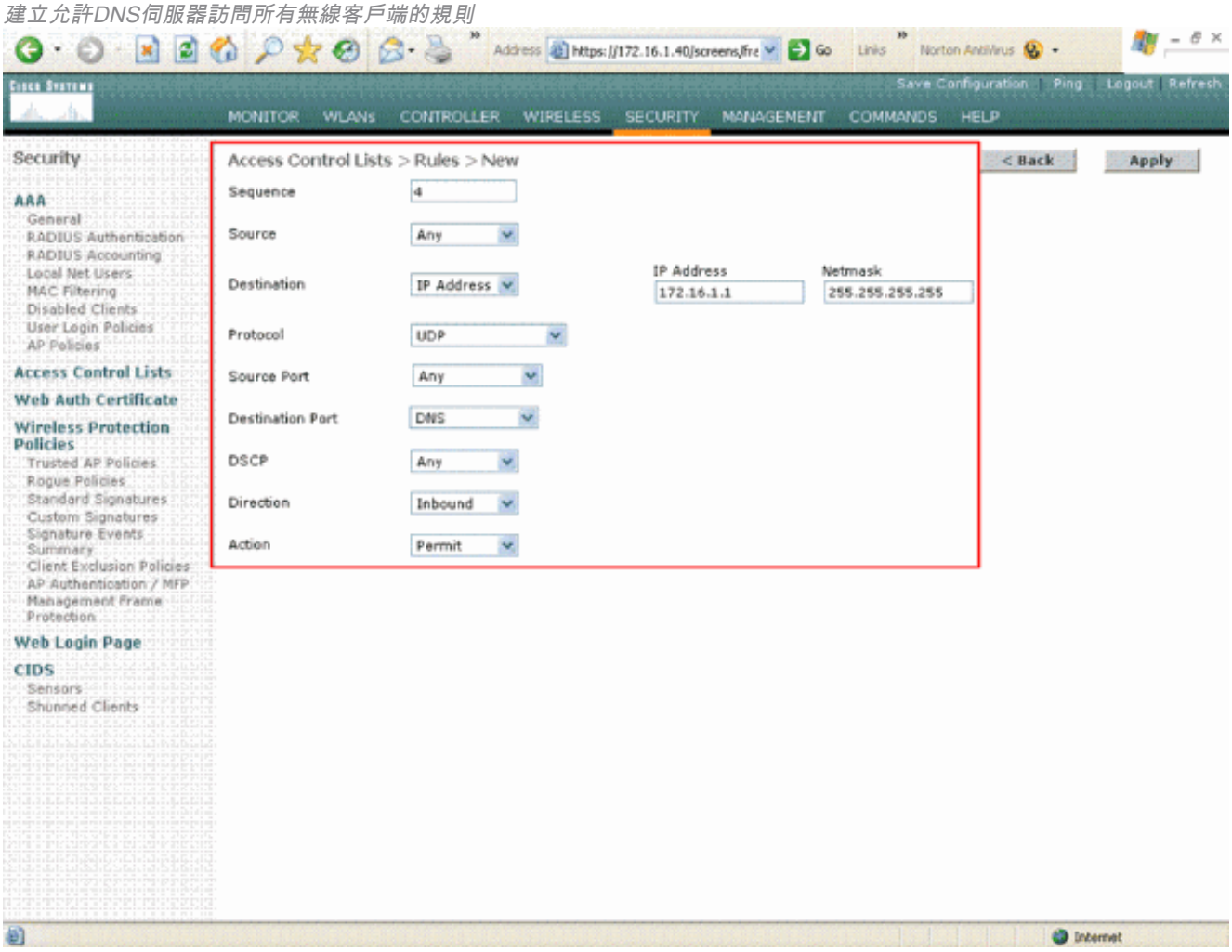


允許導致ACL允許從DHCP伺服器到無線客戶端的DHCP資料包

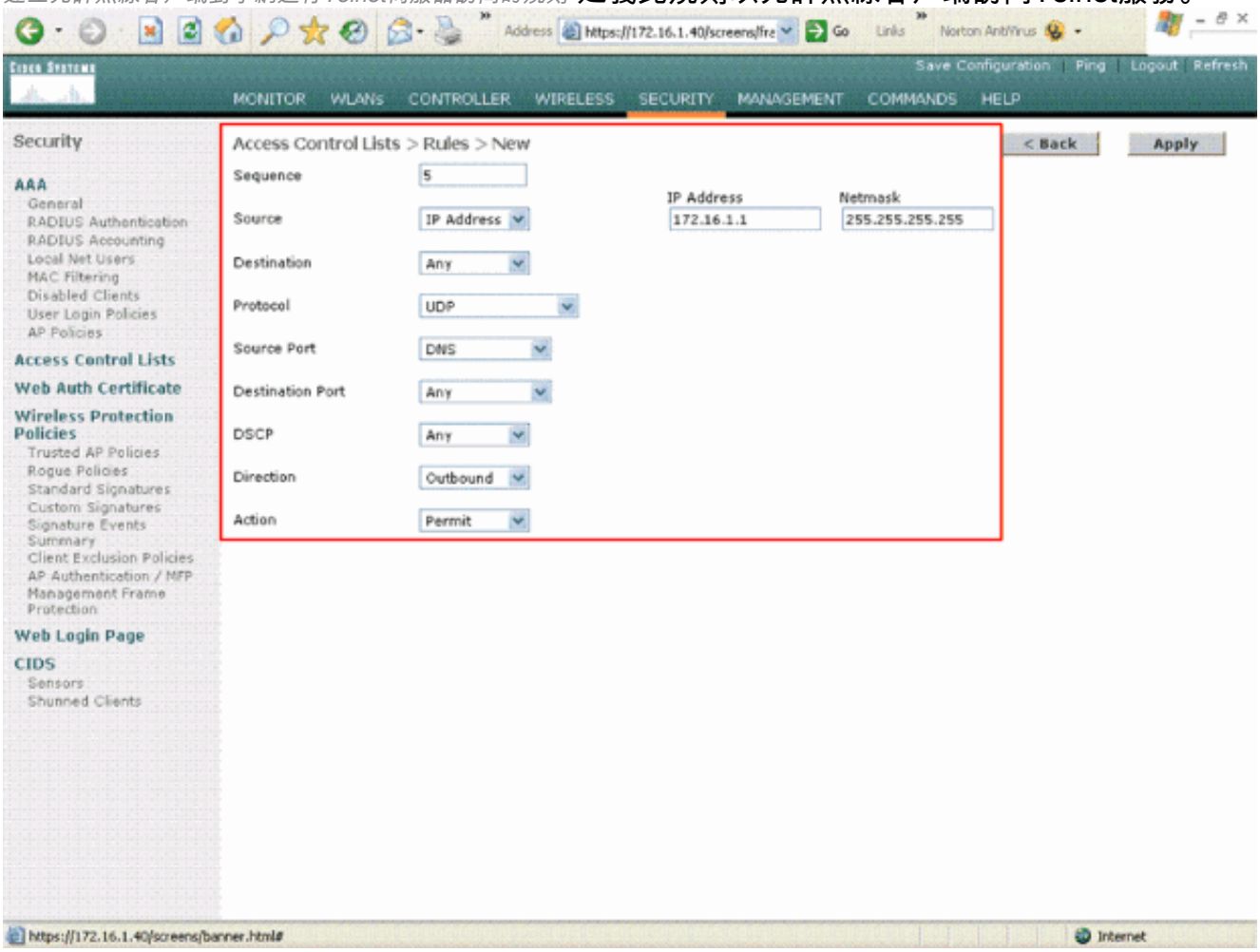
3. 類似地，建立允許DNS伺服器訪問所有無線客戶端以及無線客戶端訪問特定子網的Telnet伺服器訪問的規則。以下是範例。



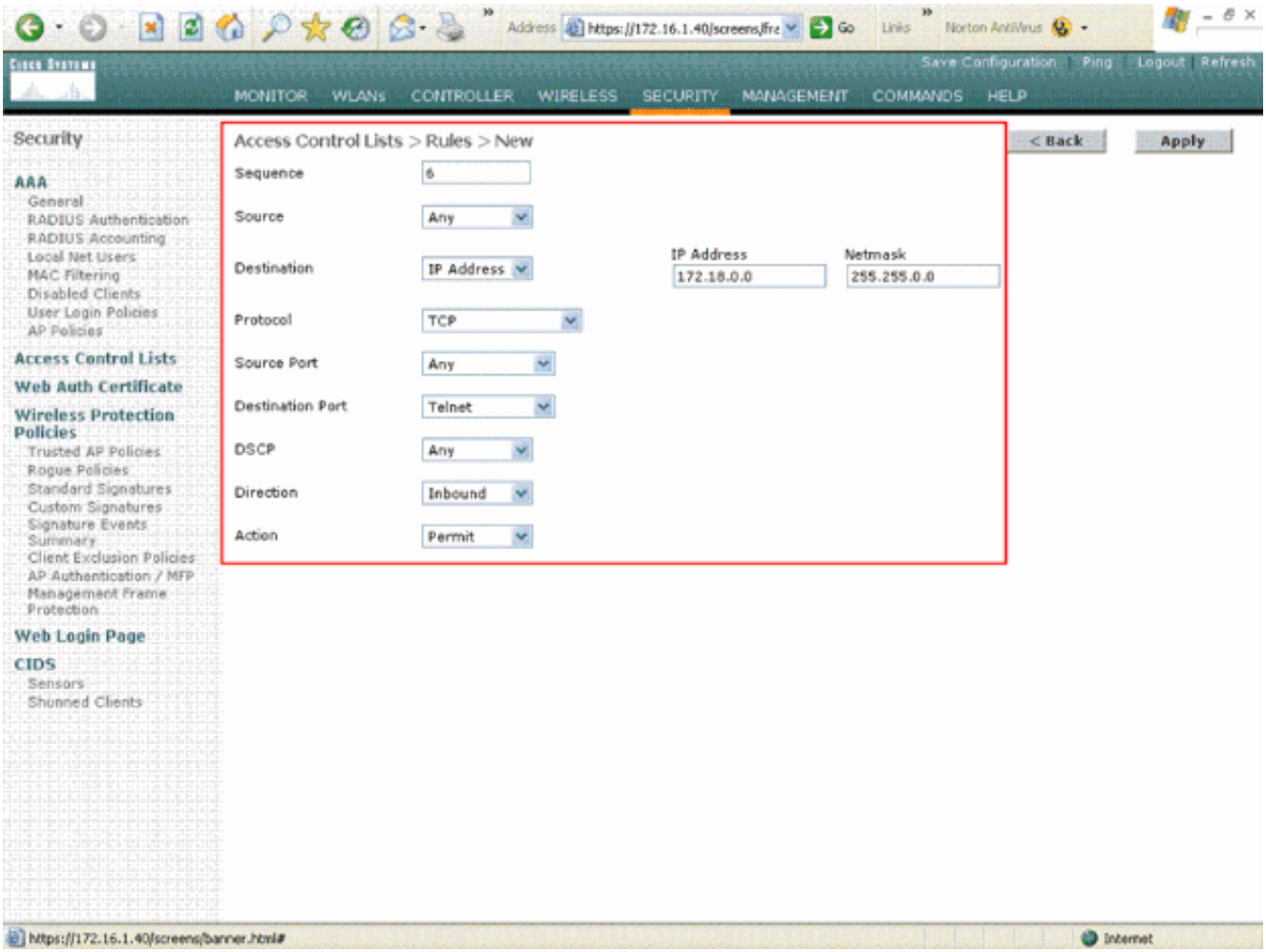
建立允許DNS伺服器訪問所有無線客戶端的規則



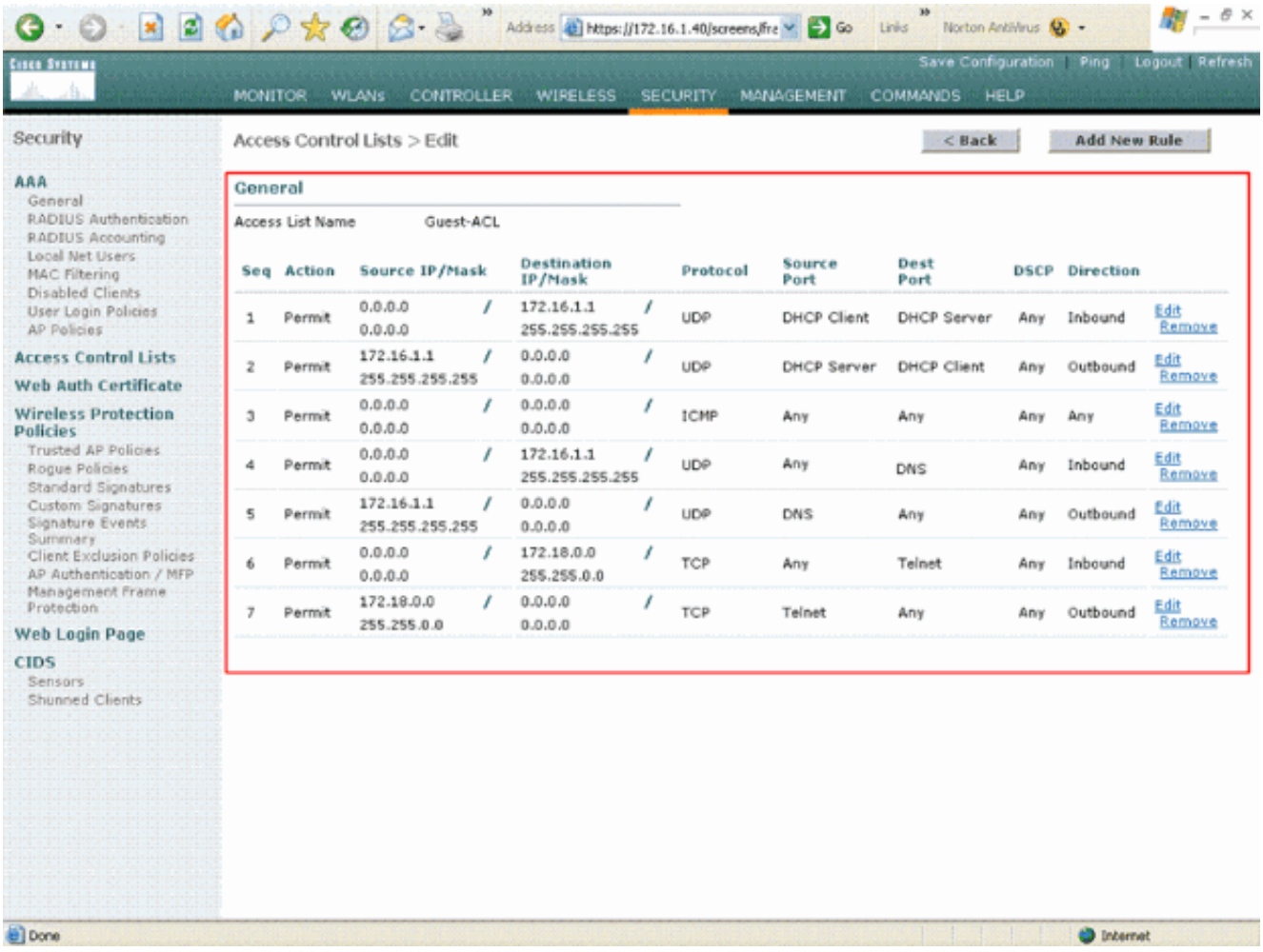
建立允許無線客戶端對子網進行Telnet伺服器訪問的規則 **定義此規則以允許無線客戶端訪問Telnet服務。**



允許無線客戶端訪問Telnet服務

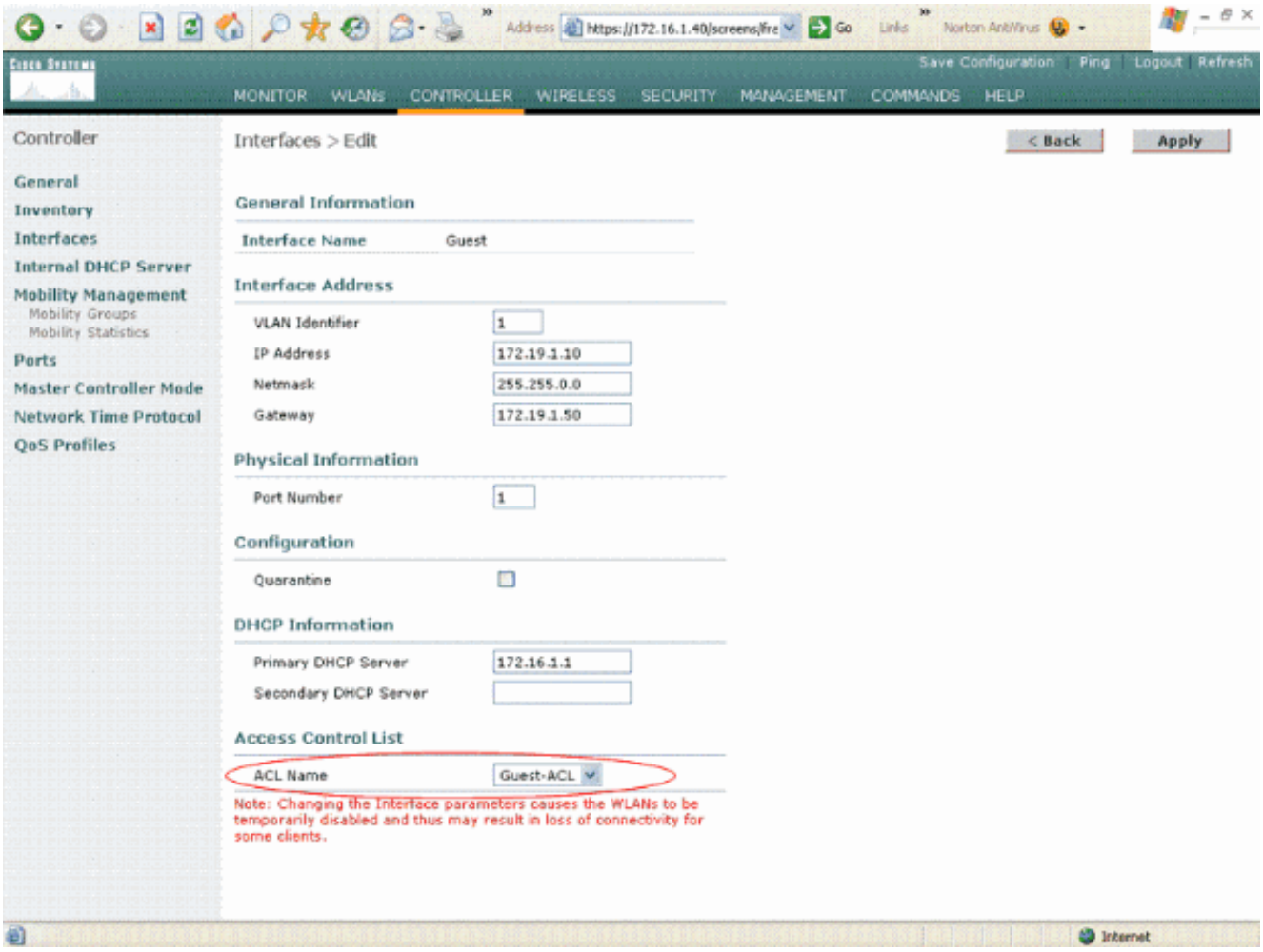


無線客戶端訪問Telnet服務的另一個示例 **ACL > Edit**頁列出為ACL定義的所有規則。



「編輯」頁列出為ACL定義的所有規則

4. 建立ACL後，需要將其應用到動態介面。若要套用ACL，請選擇**Controller > Interfaces**，然後編輯要套用ACL的介面。
5. 在動態**介面的Interfaces > Edit**頁中，從Access Control Lists下拉選單中選擇適當的ACL。以下提供範例。



從訪問控制清單選單中選擇適當的ACL

完成上述步驟後，ACL會在使用此動態介面的WLAN上允許和拒絕流量（根據已設定的規則）。介面ACL只能應用於處於連線模式的H-Reap AP，而不能應用於獨立模式。

附註：本文件假設 WLAN 和動態介面均已設定。請參閱在無線LAN控制器上設定VLAN或有關如何在WLC上建立動態介面的資訊。

配置CPU ACL

以前，WLC上的ACL沒有過濾LWAPP/CAPWAP資料流量、LWAPP/CAPWAP控制流量以及發往管理和AP管理器介面的移動流量的選項。為了解決此問題並過濾LWAPP和移動流量，在WLC韌體版本4.0中引入了CPU ACL。

CPU ACL的配置包括兩個步驟：

1. 配置CPU ACL的規則。
2. 在WLC上套用CPU ACL。

CPU ACL的規則必須以與其他ACL類似的方式配置。

驗證

思科建議您使用無線客戶端測試ACL配置，以確保已正確配置ACL。如果無法正常工作，請驗證ACL網頁上的ACL，並驗證您的ACL更改是否已應用到控制器介面。

您還可以使用以下**show**命令來驗證您的設定：

- **show acl summary** — 若要顯示控制器上配置的ACL，請使用**show acl summary命**令。以下是範例：

```
(Cisco Controller) >show acl summary

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

- **show acl detailedACL_Name** — 顯示有關已配置ACL的詳細資訊。以下是範例：

```
(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** — 要顯示CPU上配置的ACL，請使用**show acl cpu命**令。以下是範例：

```
(Cisco Controller) >show acl cpu

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

疑難排解

控制器軟體版本4.2.x或更高版本允許您配置ACL計數器。ACL計數器有助於確定對通過控制器傳輸的資料包應用了哪些ACL。此功能在排除系統故障時很有用。

以下控制器上提供ACL計數器：

- 4400系列
- Cisco WiSM
- Catalyst 3750G整合式無線LAN控制器交換器

若要啟用此功能，請完成以下步驟：

1. 依序選擇「**Security > Access Control Lists > Access Control Lists**」，以開啟「Access Control Lists」頁面。此頁列出為此控制器配置的所有ACL。
2. 若要檢視封包是否命中控制器上設定的任何ACL，請勾選**Enable Counters**核取方塊，然後按一下**Apply**。否則，請取消選中該覈取方塊。這是預設值。
3. 如果要清除ACL的計數器，請將游標懸停在該ACL的藍色下拉箭頭上，然後選擇**清除計數器**。

相關資訊

- 思科無線LAN控制器組態設定指南6.0版
- 在無線LAN控制器上配置VLAN
- 疑難排解輕量型 AP 無法加入 WLC 的問題
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。