

无线 LAN 控制器中的 ACL 配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[WLC 上的 ACL](#)

[在 WLC 中配置 ACL 时的注意事项](#)

[在 WLC 上配置 ACL](#)

[配置允许访客用户服务的规则](#)

[配置 CPU ACL](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文解释如何在无线 LAN 控制器 (WLC) 上配置访问控制列表 (ACL) 以过滤进入和离开 WLAN 的数据流。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 关于如何配置 WLC 和轻量级接入点 (LAP) 以满足基本运作的知识
- 基本了解轻量级接入点协议 (LWAPP) 和无线安全方法

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件 4.0 的 Cisco 2000 系列 WLC
- Cisco 1000 系列 LAP
- 运行固件版本 2.6 的 Cisco 802.11a/b/g 无线客户端适配器
- Cisco Aironet Desktop Utility (ADU) 版本 2.6

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

WLC 上的 ACL

WLC 上的 ACL 旨在限制或允许无线客户端访问其 WLAN 上的服务。

在 WLC 固件版本 4.0 前，ACL 绕过管理接口，因此除了阻止无线客户端通过 **Management Via Wireless** 选项管理控制器以外，您无法影响发送到 WLC 的数据流。所以，ACL 只能应用到动态接口。在 WLC 固件版本 4.0 中有能过滤发送到管理接口的数据流的 CPU ACL。后文将提供如何[配置 CPU ACL](#) 的示例。

您最多能定义 64 个 ACL，每个有 64 个规则（或过滤器）。每个规则有影响其操作的参数。当数据包匹配规则的所有参数时，为该规则设置的操作将应用到数据包。您能通过 GUI 或 CLI 配置 ACL。

以下是您在 WLC 上配置 ACL 时应理解的规则：

- 如果源和目标为 **any**，则 ACL 应用到的目标可以为 **any**。
- 如果源或目标为 **not any**，则必须指定过滤器方向，并且必须创建相反方向的逆向语句。
- WLC 对入站与出站的感知并非是直观的。它是从面向无线客户端的 WLC 角度，而不是从客户端的角度。因此，入站方向意味着数据包从无线客户端发往 WLC，而出站方向意味着从 WLC 退出到无线客户端的数据包。
- ACL 末尾存在隐式拒绝。

在 WLC 中配置 ACL 时的注意事项

WLC 中的 ACL 与路由器中 ACL 工作方式不同。在 WLC 中配置 ACL 时需要记住以下事项：

- 当您打算拒绝或允许 IP 数据包通过时，最容易犯的错误是选择 IP。由于您选择了 IP 数据包里面的内容，将导致拒绝或允许 IP-in-IP 数据包。
- 控制器 ACL 不能阻止 1.1.1.1（虚拟 IP 地址），也无法阻止无线客户端的 DHCP 信息包。
- 控制器 ACL 不能阻塞被注定给无线客户端从有线网络接收的组播数据流。控制器 ACL 为从无线客户端初始化的组播数据流处理，被注定对有线网络或其他无线客户端同一个控制器的。
- 不同于路由器，ACL 应用到接口后可在两个方向控制数据流，但它不执行状态防火墙。如果忘记在 ACL 中开一个口子以便返回数据流，则将引发问题。
- 控制器 ACL 仅阻止 IP 信息包。您不能阻止第 2 层或第 3 层的非 IP 数据包。
- 控制器 ACL 不使用类似路由器的反掩码。这里的 255 表示准确匹配该 IP 地址的八位组。
- 控制器上的 ACL 在软件中完成并影响转发性能。

注意： 如果将 ACL 应用到接口或 WLAN，无线吞吐量会降低并且可能导致潜在的丢包。为了提高吞吐量，请从接口或 WLAN 上删除 ACL 并且将 ACL 移至相邻的有线设备。

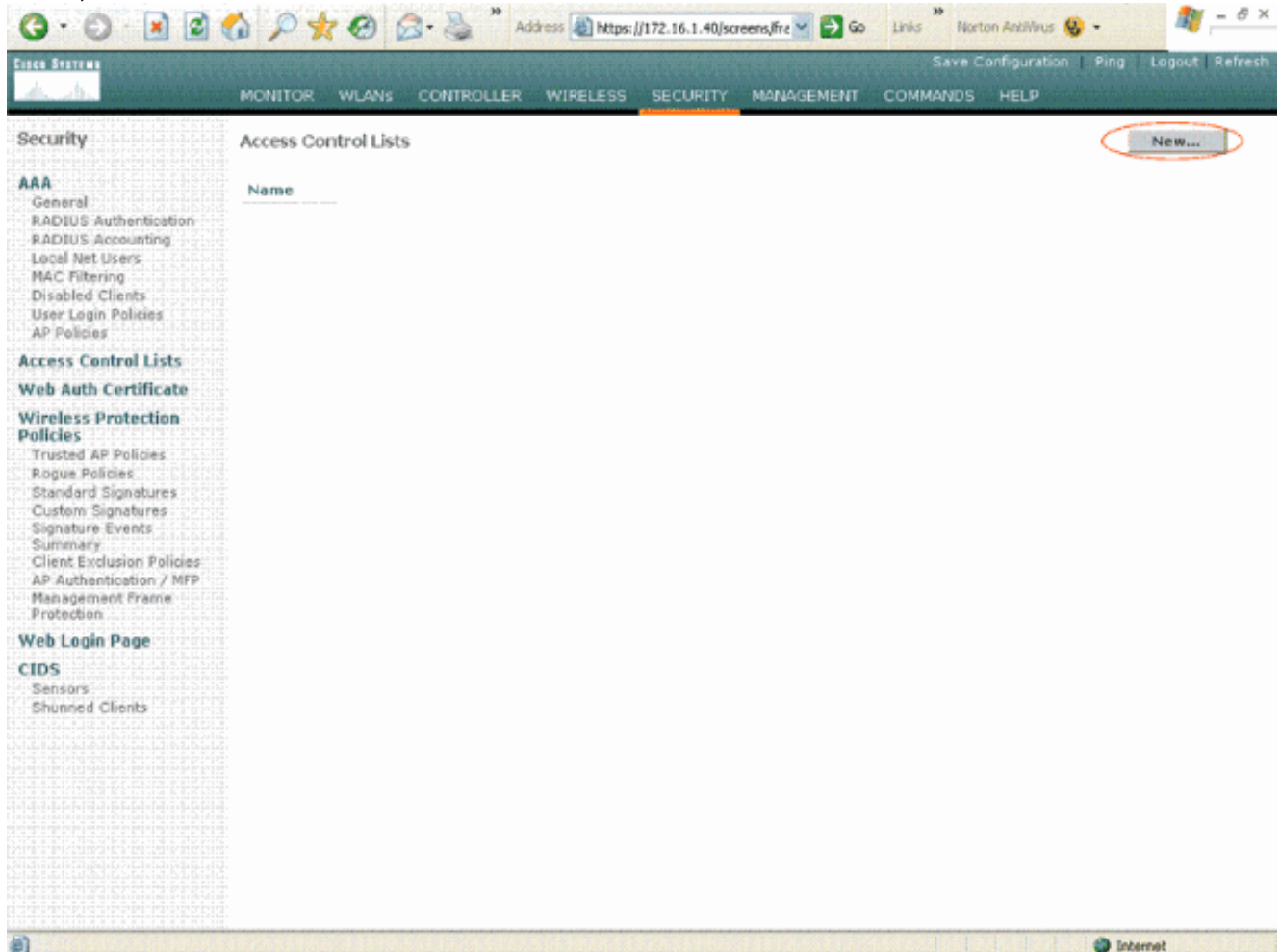
在 WLC 上配置 ACL

此部分描述如何在 WLC 上配置 ACL。目标是配置允许访客客户端访问这些服务的 ACL：

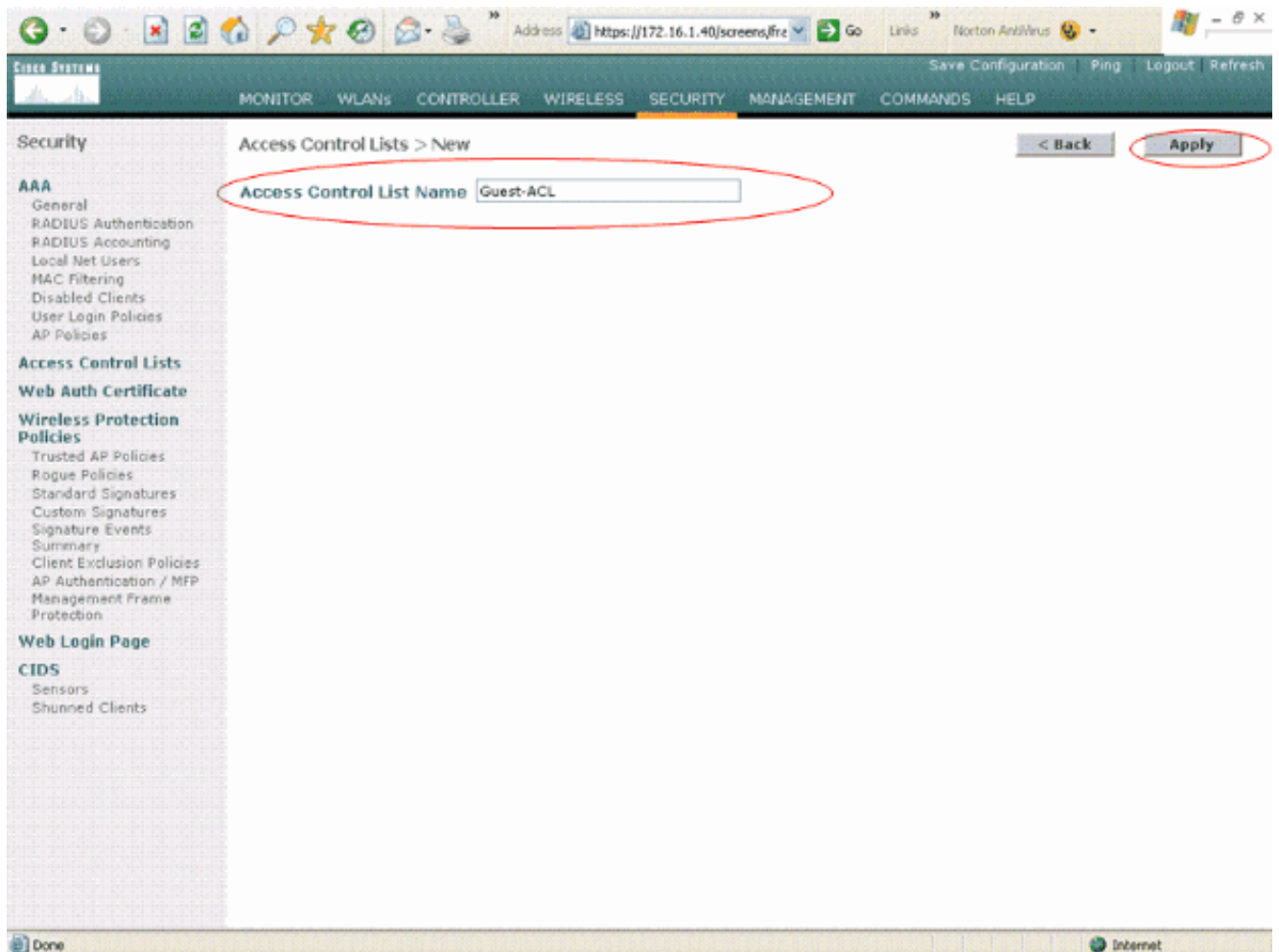
- 无线客户端和 DHCP 服务器之间的动态主机配置协议 (DHCP)
- 网络中所有设备之间的 Internet 控制消息协议 (ICMP)
- 无线客户端和 DNS 服务器之间的域名系统 (DNS)
- 特定子网的 Telnet

必须为无线客户端阻塞所有其他服务。完成下列步骤以使用 WLC GUI 创建 VPN 隧道：

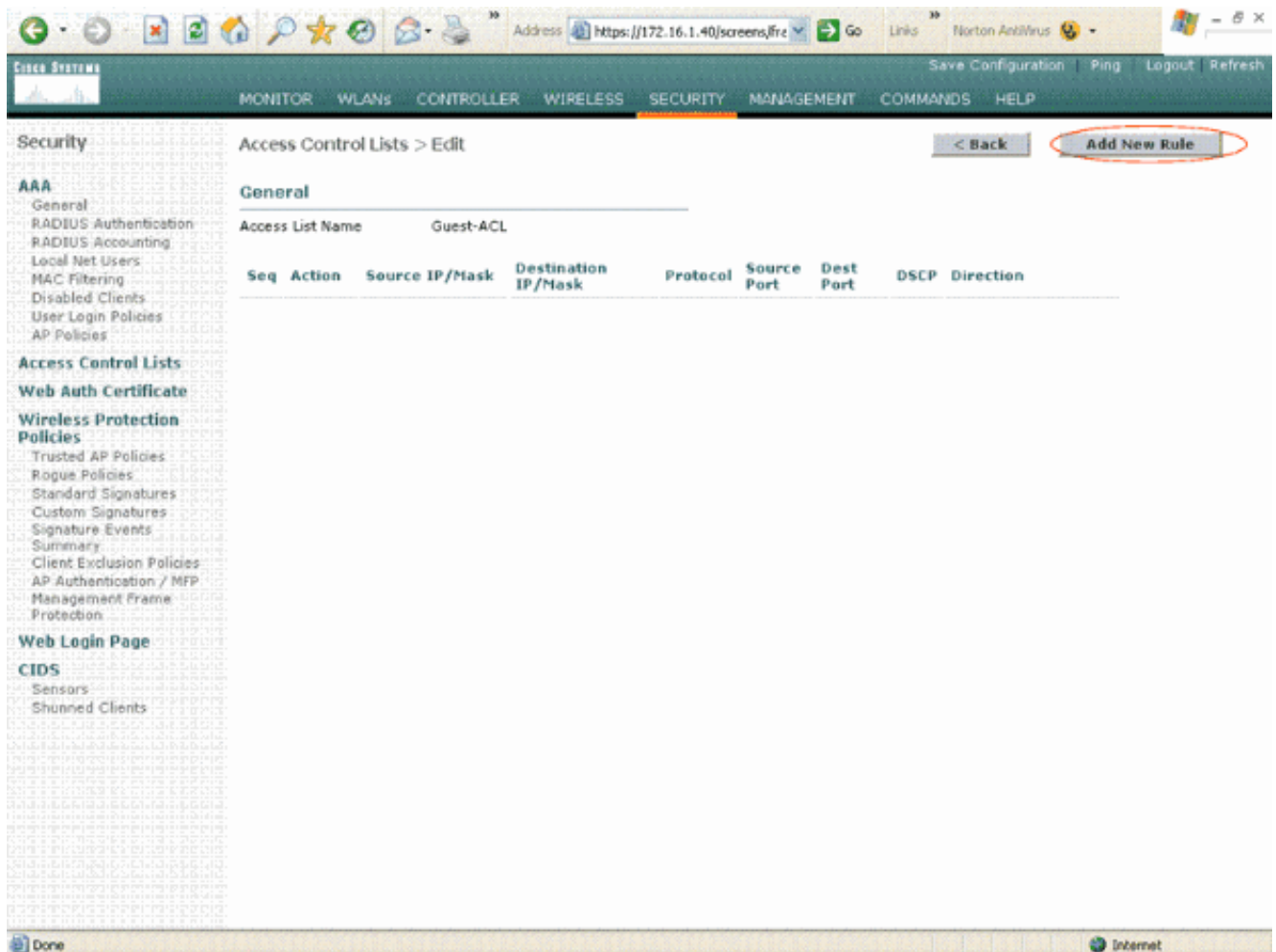
1. 转到 WLC GUI 并选择 **Security > Access Control Lists**。出现 Access Control Lists 页。此页列出了在 WLC 上配置的 ACL。您也可以利用它编辑或删除其中任一 ACL。要创建新的 ACL，请单击 **New**。



2. 输入 ACL 的名称并单击 **Apply**。最多可以输入 32 个字母数字字符。在本例中，ACL 的名称是 **Guest-ACL**。创建 ACL 后，单击 **Edit** 创建 ACL 的规则。



3. 当 Access Control Lists > Edit 页出现时，单击 **Add New Rule**。出现 Access Control Lists > Rules > New 页。



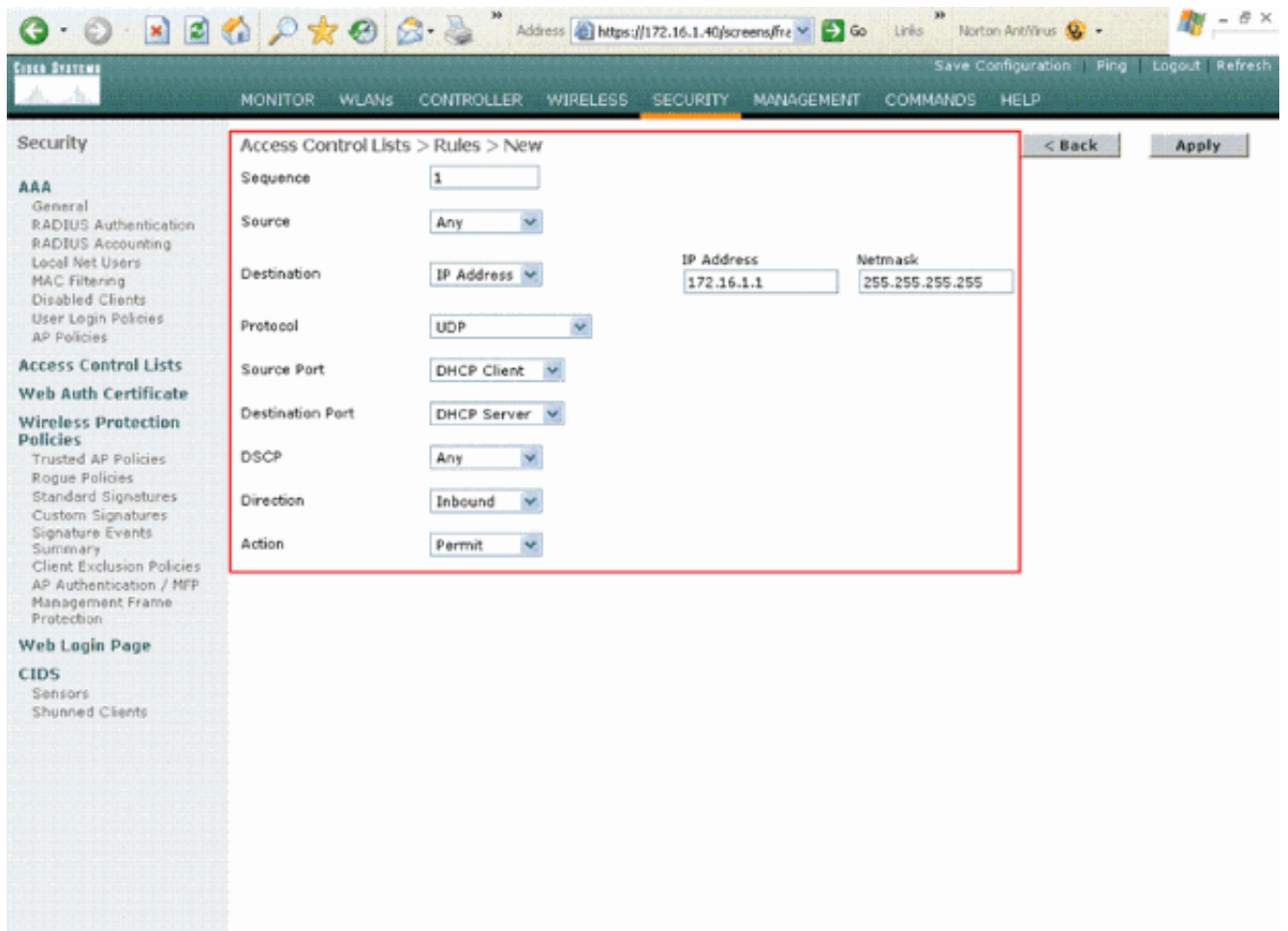
4. 配置允许访客用户使用这些服务的规则：无线客户端和 DHCP 服务器之间的 DHCP 网络中所有设备之间的 ICMP 无线客户端和 DNS 服务器之间的 DNS 特定子网的 Telnet

[配置允许访客用户服务的规则](#)

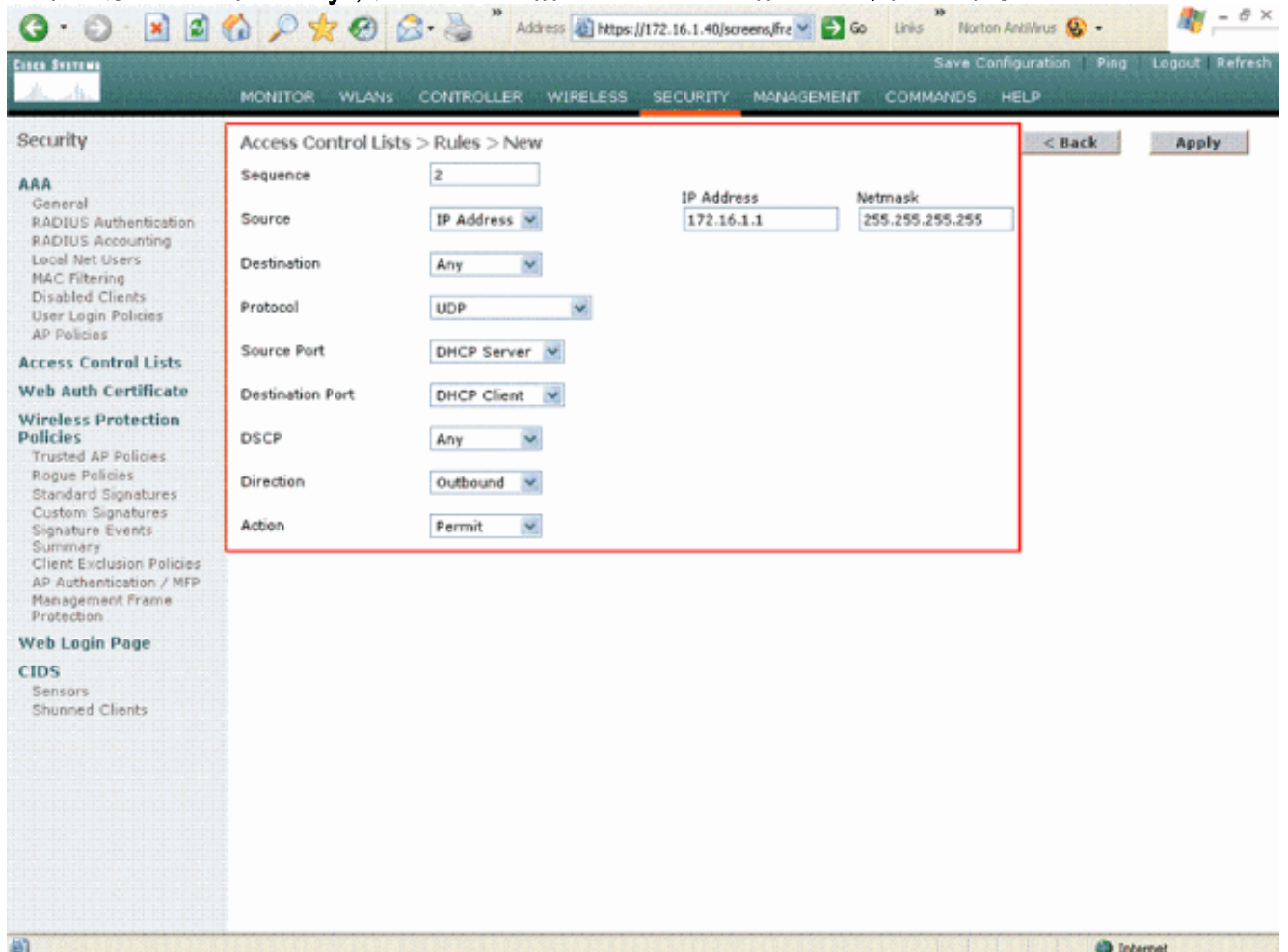
此部分给出了如何为以下服务配置规则的示例：

- 无线客户端和 DHCP 服务器之间的 DHCP
- 网络中所有设备之间的 ICMP
- 无线客户端和 DNS 服务器之间的 DNS
- 特定子网的 Telnet

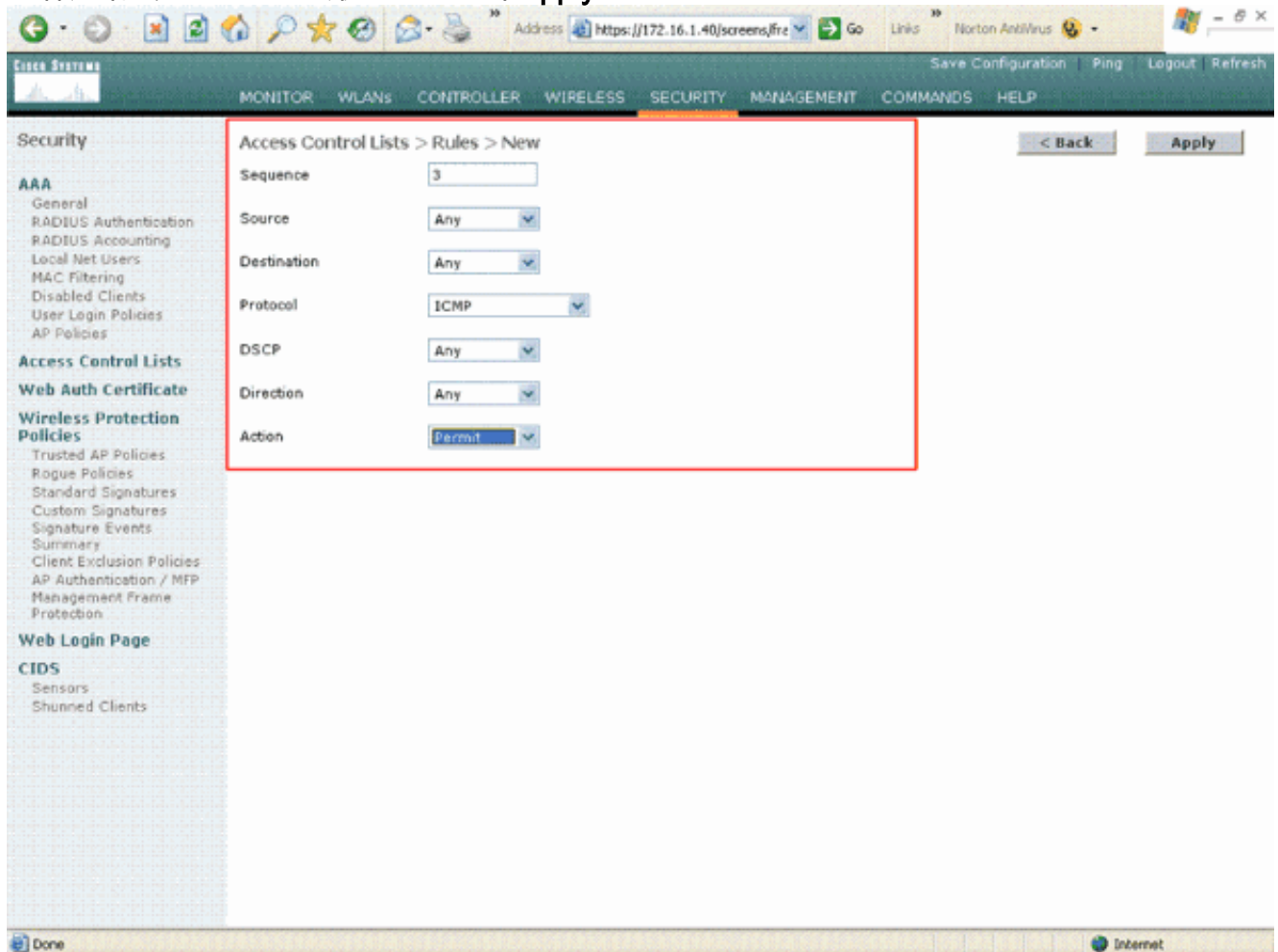
1. 为了定义 DHCP 服务的规则，请选择来源和目标 IP 范围。此示例使用 **any** 来源，这意味着允许任意无线客户端访问 DHCP 服务器。在本例中，服务器 172.16.1.1 作为 DHCP 和 DNS 服务器。因此，目标 IP 地址是 172.16.1.1/255.255.255.255 (带主机掩码)。由于 DHCP 是基于 UDP 的协议，请从 Protocol 下拉字段中选择 **UDP**。如果您在上一步中选择了 TCP 或 UDP，则会出现另外两个参数：来源端口和目标端口。指定来源及目标端口详细信息。对于此规则，来源端口是 **DHCP 客户端**，并且目标端口是 **DHCP 服务器**。选择 ACL 将应用的方向。由于此规则是从客户端到服务器，所有此示例使用 **入站**。从 Action 下拉框中选择 **Permit** 让此 ACL 允许 DHCP 数据包从无线客户端发送到 DHCP 服务器。默认值是“Deny”。单击 **Apply**。



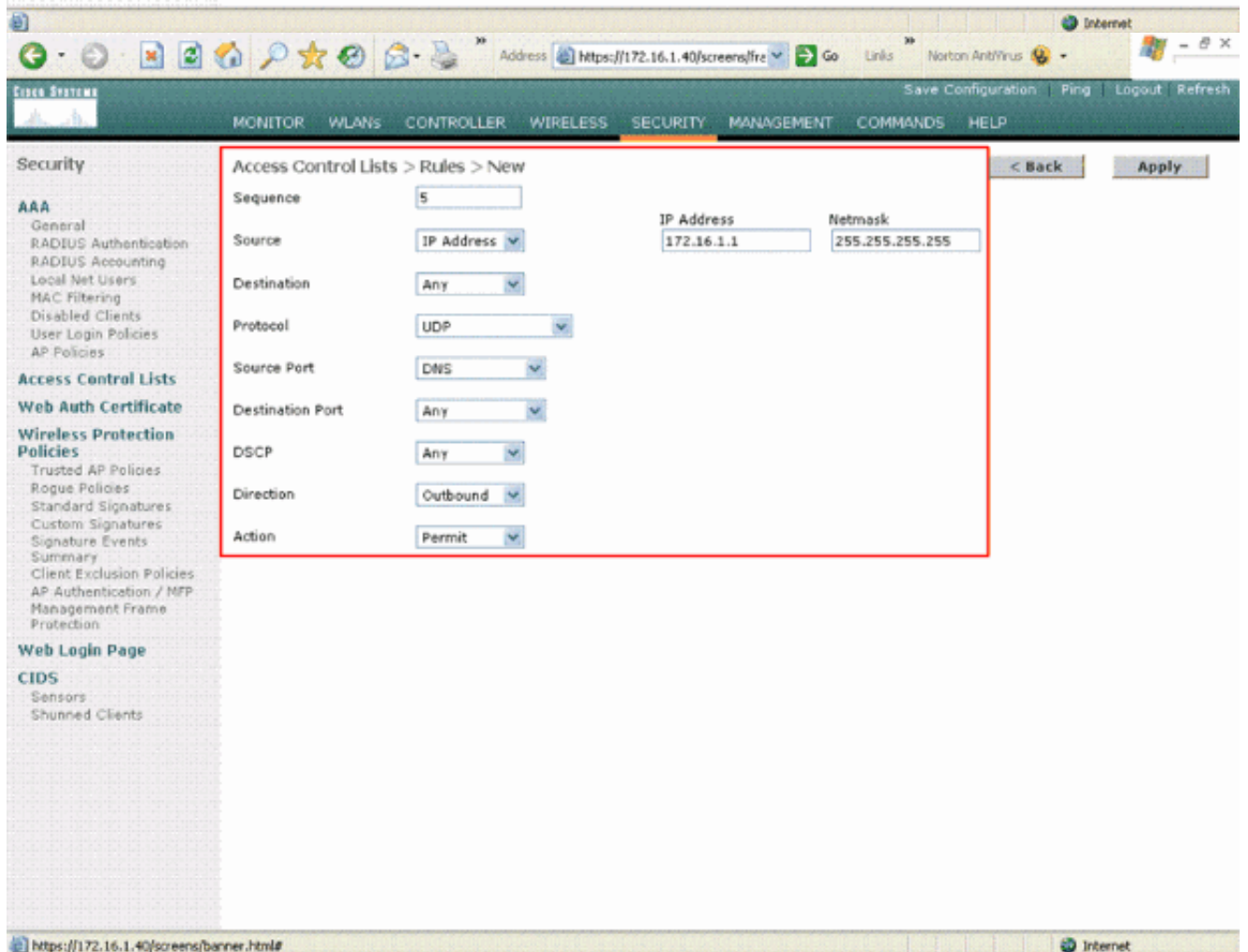
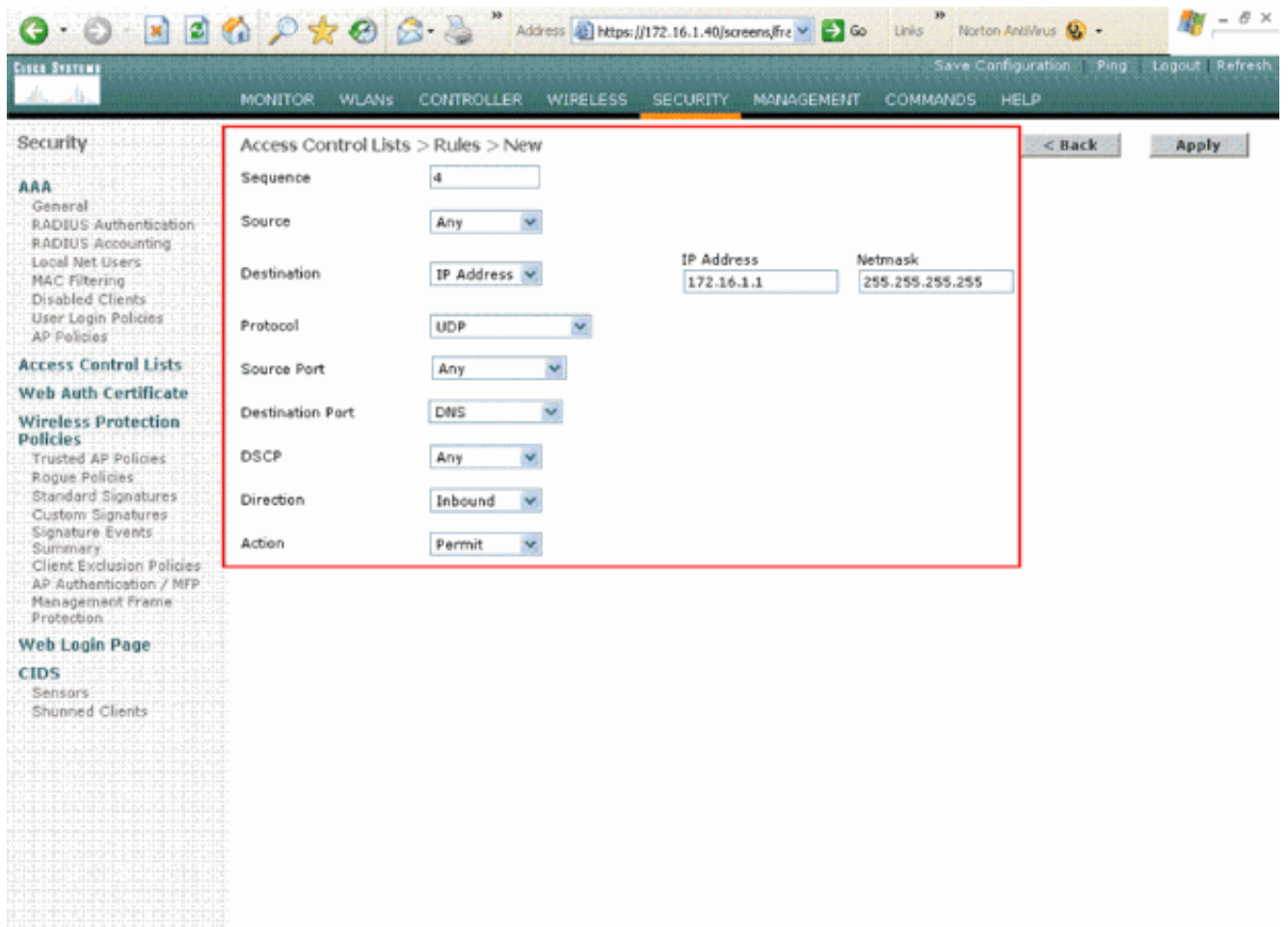
如果来源和目标不是 any，则必须创建相反方向的逆向语句。下面是一个示例。



2. 为了定义规则以允许 ICMP 数据包在所有设备之间传输，请在 Source 和 Destination 字段中选择 **any**。这是默认值。从 Protocol 下拉式字段中选择 **ICMP**。由于此示例在 Source 和 Destination 字段中使用 **any** 字段，因此您无需指定方向。可以保留默认值 **any**。并且无需创建相反方向的逆向语句。从 Action 下拉框中选择 **Permit**，让此 ACL 允许 DHCP 数据包从无线客户端发送到 DHCP 服务器。单击 **Apply**。



3. 同样，请创建规则允许 DNS 服务器访问所有无线客户端以及允许无线客户端的 Telnet 服务器访问特定子网。以下是一些示例：



定义此规则以允许无线客户端访问 Telnet 服务。

The screenshot shows the Cisco Systems configuration interface for "Access Control Lists > Rules > New". The configuration is as follows:

Sequence	6	
Source	Any	
Destination	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	

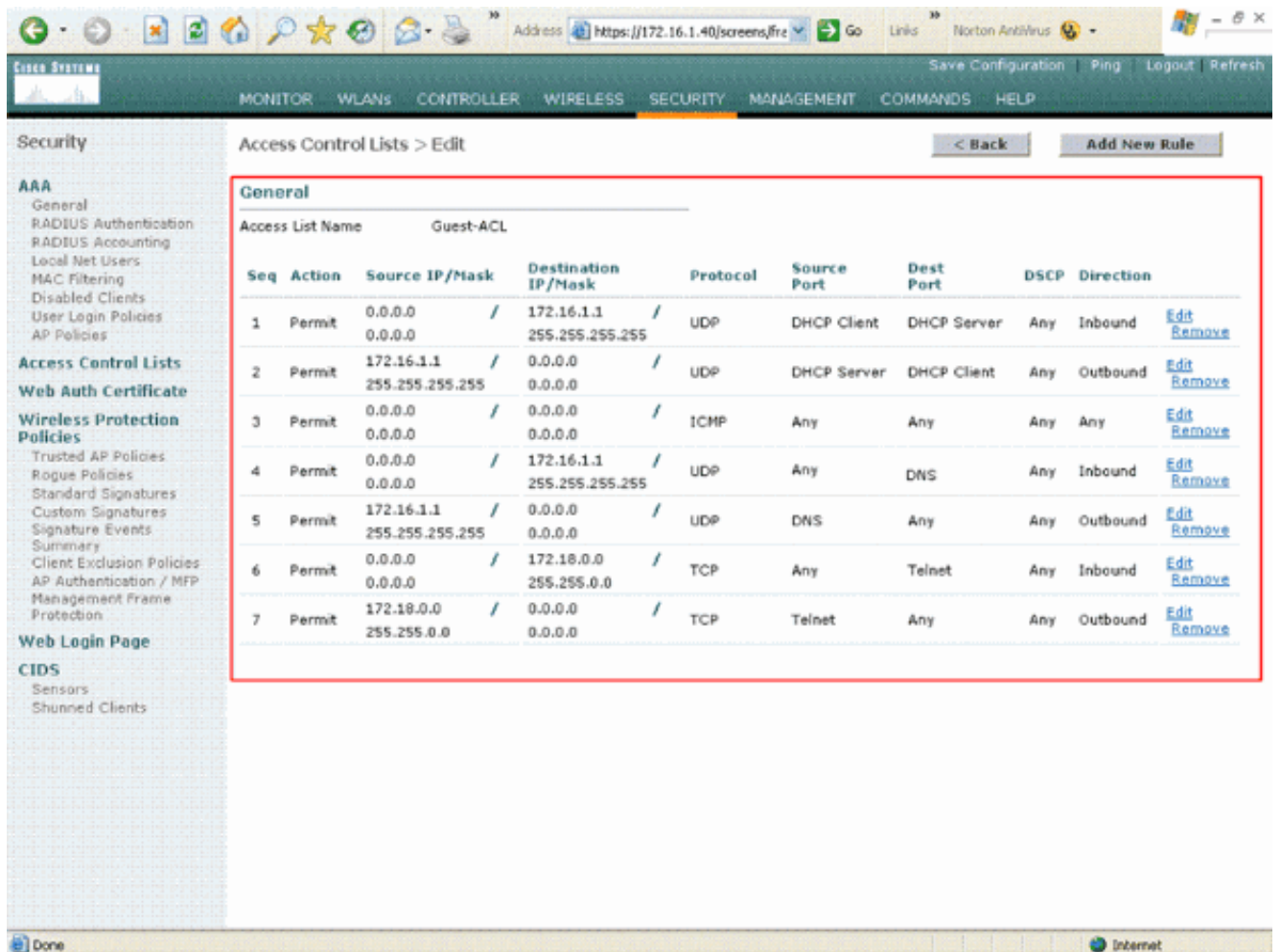
Navigation buttons: < Back, Apply

The screenshot shows the Cisco Systems configuration interface for "Access Control Lists > Rules > New". The configuration is as follows:

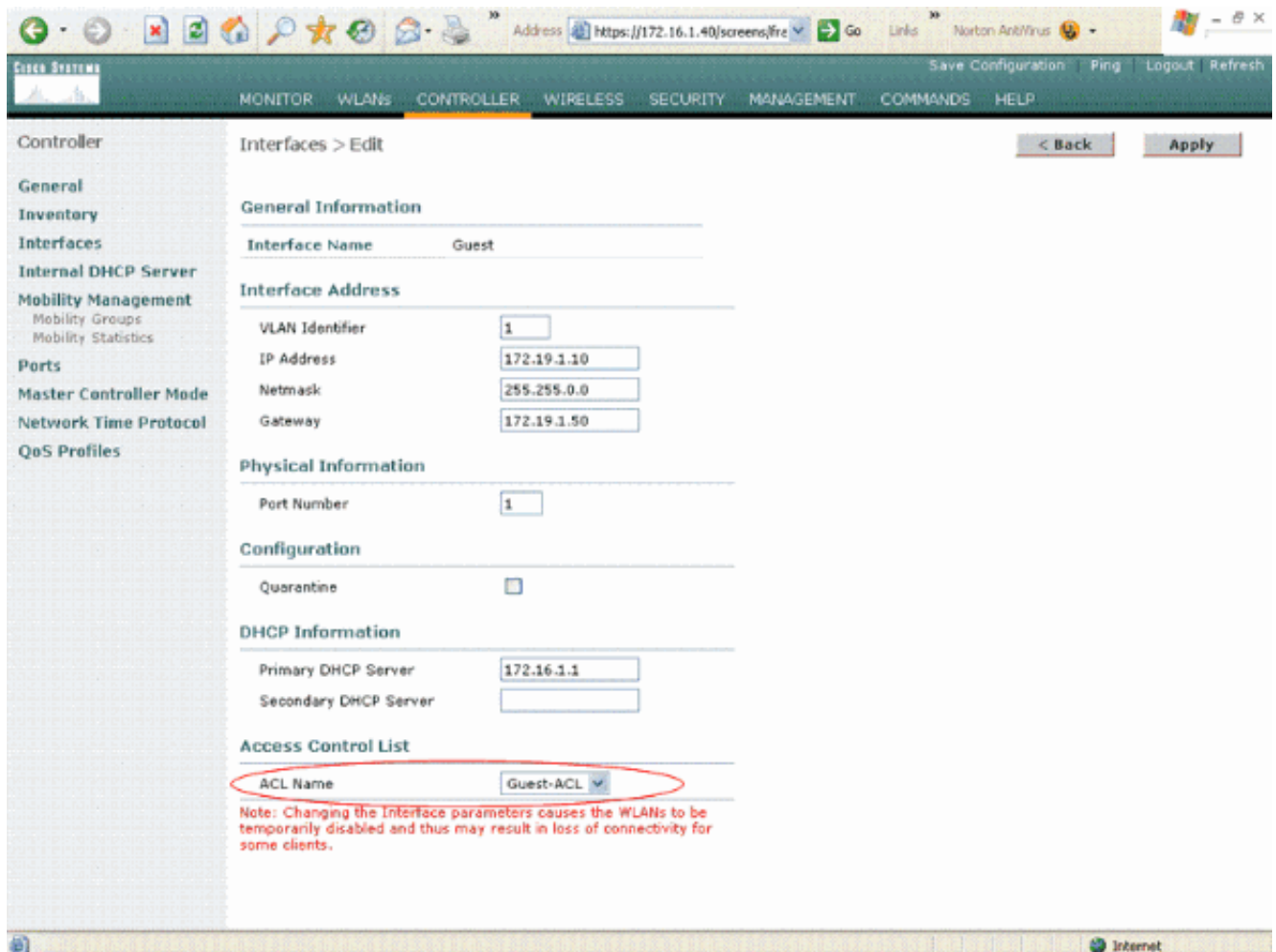
Sequence	7	
Source	IP Address	
Destination	Any	
Protocol	TCP	
Source Port	Telnet	
Destination Port	Any	
DSCP	Any	
Direction	Outbound	
Action	Permit	

Navigation buttons: < Back, Apply

ACL > Edit 页列出了为此 ACL 定义的所有规则。



4. ACL 创建后，需要应用到动态接口。为了应用 ACL，请选择 **Controller > Interfaces** 并且编辑您要应用 ACL 的接口。
5. 在动态接口的 **Interfaces > Edit** 页，从 Access Control Lists 下拉菜单中选择适当的 ACL。下面是一个示例。



完成后，ACL 允许或拒绝使用此动态接口的 WLAN 上的数据流（根据配置的规则）。接口 ACL 只能在连续模式中应用到 H-Reap AP，而非独立模式。

注意：有关如何在 WLC 上通过 CLI 创建 ACL，请参阅[使用 CLI 配置访问控制列表](#)。

注意：本文假设已配置 WLAN 和动态接口。有关如何在 WLC 上创建动态接口的信息，请参阅[无线 LAN 控制器上的 VLAN 配置示例](#)。

配置 CPU ACL

以前，WLC 上的 ACL 没有选项来过滤发送到管理和 AP 管理器接口的 LWAPP/CAPWAP 数据流、LWAPP/CAPWAP 控制数据流和移动数据流。为了解决此问题并过滤 LWAPP 和移动数据流，WLC 固件版本 4.0 引入了 CPU ACL。

CPU ACL 的配置包括两个步骤：

1. CPU ACL 的配置规则。
2. 在 WLC 上应用 CPU ACL。

CPU ACL 的规则应与其他 ACL 采用同样的配置方法。有关 CPU ACL 的详细信息，请参阅[保护无线 LAN 控制器 \(WLC\) 的 CPU ACL 部分](#)。

验证

Cisco 建议您使用无线客户端测试您的 ACL 配置以确保正确配置。如果不能正确运行，请验证 ACL 网页上的 ACL 并验证 ACL 更改应用到控制器接口。

您也可使用这些 **show** 命令验证您的配置：

- **show acl summary** — 为了显示在控制器上配置的 ACL，请使用 **show acl summary** 命令。示例如下：

```
(Cisco Controller) >show acl summary
```

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

- **show acl detailed ACL_name** — 显示已配置 ACL 的详细信息。示例如下：

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

Dest Port	Source	Destination	Source 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** — 为了显示 CPU 上配置的 ACL，请使用 **show acl cpu** 命令。示例如下：

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

Dest Port	Source	Destination	Source 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		

故障排除

您可在控制器软件版本 4.2.61.0 或更新版本中配置 ACL 计数器。ACL 计数器能协助确定哪些 ACL

应用到通过控制器传送的数据包中。当您对系统进行故障排除时此功能非常有用。

ACL 计数器在这些控制器上可用：

- 4400 系列
- Cisco WiSM
- Catalyst 3750G 集成无线局域网控制器交换机

要启用此功能，请完成以下步骤：

1. 选择 **Security > Access Control Lists > Access Control Lists** 以打开 Access Control Lists 页。此页列出了为此控制器配置的所有 ACL。
2. 为查看数据包是否到达您控制器上配置的任一 ACL，选中 **Enable Counters** 复选框并且单击 **Apply**。否则，请保留复选框空白。这是默认值。
3. 如果要清除 ACL 的计数器，将光标停留在该 ACL 的蓝色下拉箭头上，并选择 **Clear counters**。

[相关信息](#)

- [配置和应用访问控制列表](#)
- [无线局域网控制器上的 VLAN 配置示例](#)
- [轻量 AP \(LAP\) 注册到无线 LAN 控制器 \(WLC\)](#)
- [Cisco 无线 LAN 控制器配置指南 4.0 版](#)
- [无线/移动性技术支持](#)
- [技术支持和文档 - Cisco Systems](#)