无线控制器ACL配置实例

文档 ID: 71978

介绍

本文档介绍如何在无线控制器（WLC）上配置访问控制列表（ACL）来过滤进入和离开无线局域网的流量。

前提

要求

在尝试配置前，确保你满足如下的要求：

- 具备配置无线控制器和轻量级无线接入点进行基本工作的知识
- 具备轻量级无线接入点协议（LWAPP）和无线安全方法的基本知识

使用的设备

本文档中的信息基于如下的软件和硬件版本：

- 思科2000系列无线控制器，固件版本4.0
- 思科1000系列轻量线无线接入点
- 思科802.1 1a/b/g无线网卡，固件版本2.6
- 思科Aironet Desktop Utility (ADU)，版本2.6

本文档中的信息来自特定实验环境的设备。文档中所有的相关设备都是从默认配置开始的。如果你的网络环境是在线的，确保要了解任何一条命令的潜在影响。

惯例

要了解更多文档惯例的信息，请参见思科技术提示惯例。

无线控制器ACL

无线控制器上的ACL用于限制或允许无线客户端访问无线局域网内的服务。

在无线控制器固件版本4.0之前，ACL在Management Interface上是旁路的，所以你不能影响去往无线控制器的流量，除非通过**Management Via Wireless**的选项来避免无线客户端管理控制器。因此，ACL只能用于动态的Interface。在无线控制器固件版本4.0中，有CPU ACL可以过滤去往Management Interface的流量。如何配置CPU ACL的例子稍后会在文档中列出。

你可以定义最多64个ACL，每个ACL最多64条规则。每条规则有影响行为的参数。当一个数据包匹配了一条规则的所有参数，相应的行为就会运用到这个数据包上。你可以通过GUI或CLI配置ACL。

在配置无线控制器ACL前，你需要了解一些规则：

- 如果源和目的都是**any,** 则这个ACL的方向可以是**any.**
- 如果源或目的之一不是**any,** 那么过滤器的方向必须指定，并且反方向的相反语句必须定义。
- 无线控制器的inbound和outbound方向概念并非直观上的。它是从无线控制器面向无线客户端的角度看的，并非从无线客户端的角度。因此，inbound方向是指数据包从无线客户端进入无线控制器，outbound方向是指数据包从无线控制器出去到无线客户端去。
- 在ACL的末尾有隐式的deny。

无线控制器上配置ACL需注意

无线控制器上的ACL与路由器上的工作是不一样的。当你在无线控制器上配置ACL时，有一些事项要注意：

- 当你想要拒绝或允许IP的数据包时，最常见的错误是选择IP。因为你选择的是IP数据包里面的内容，这样就导致拒绝或允许IP数据包内的IP信息。
- 控制器的ACL无法禁止1.1.1.1（virtual IP地址），因此无法禁止无线客户端的DHCP包。
- 控制器的ACL无线禁止组播和广播的数据包，因为这些包是发送到无线接入点的management interface上的。
- 不像路由器那样，ACL应用到端口上后会控制双向的流量。如果你忘记了在回来的数据流的ACL上打开策略，就会导致出问题。
- 控制器的ACL只能禁止IP数据包。你不能禁止2层的ACL或3层的非IP的数据包。
- 控制器的ACL不像路由器那样用反掩码。在这里，255的意思是完全匹配IP地址的8位数字。
- 控制器的ACL是由软件实现的。

配置无线控制器ACL

本章节描述如何在无线控制器上配置ACL。目标是配置ACL允许访客访问如下的服务：

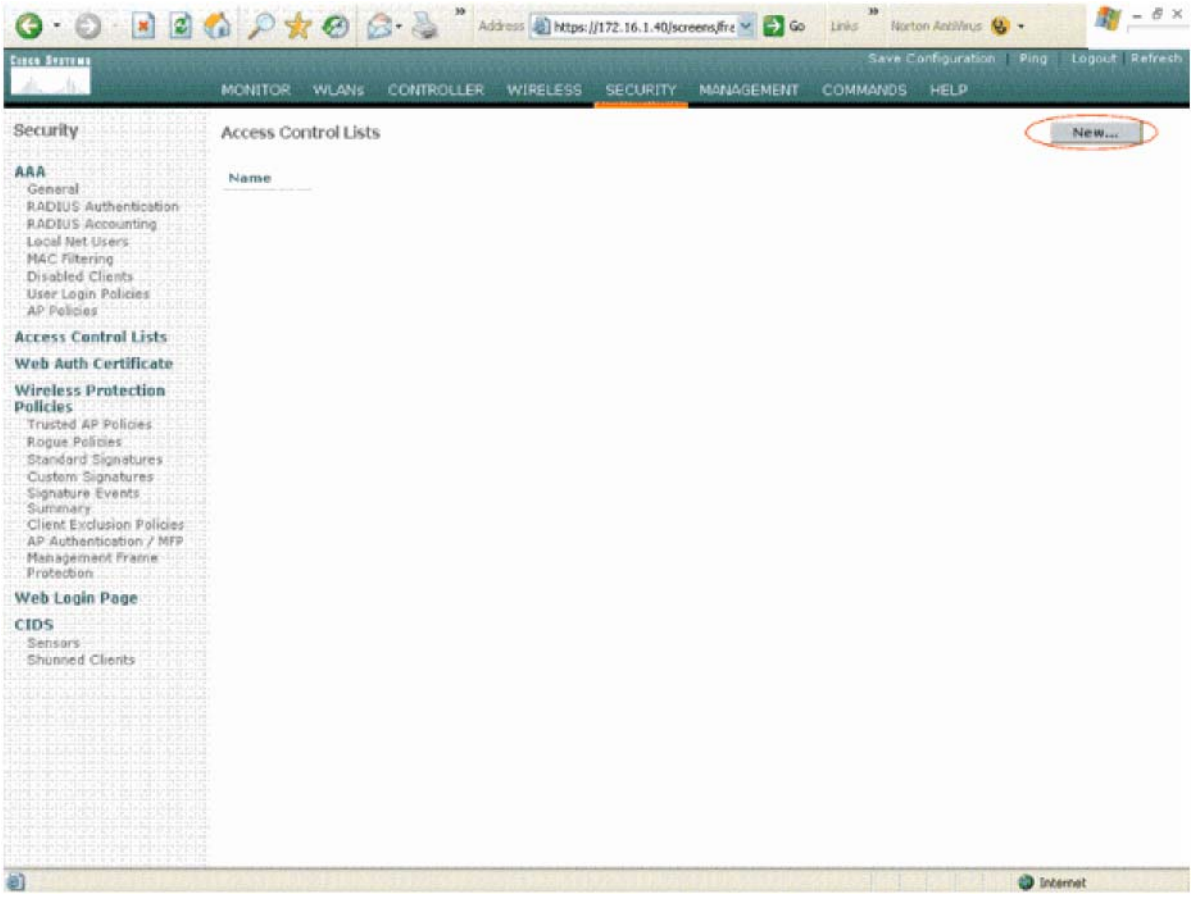
- 无线客户端与DHCP服务器之间的DHCP数据
- 网络中所有的设备之间的ICMP数据
- 无线客户端与DNC服务器之间的DNS数据

- Telnet服务到特定的子网

无线客户端的所有其他服务都必须被禁止。根据如下步骤，用无线控制器GUI配置ACL：

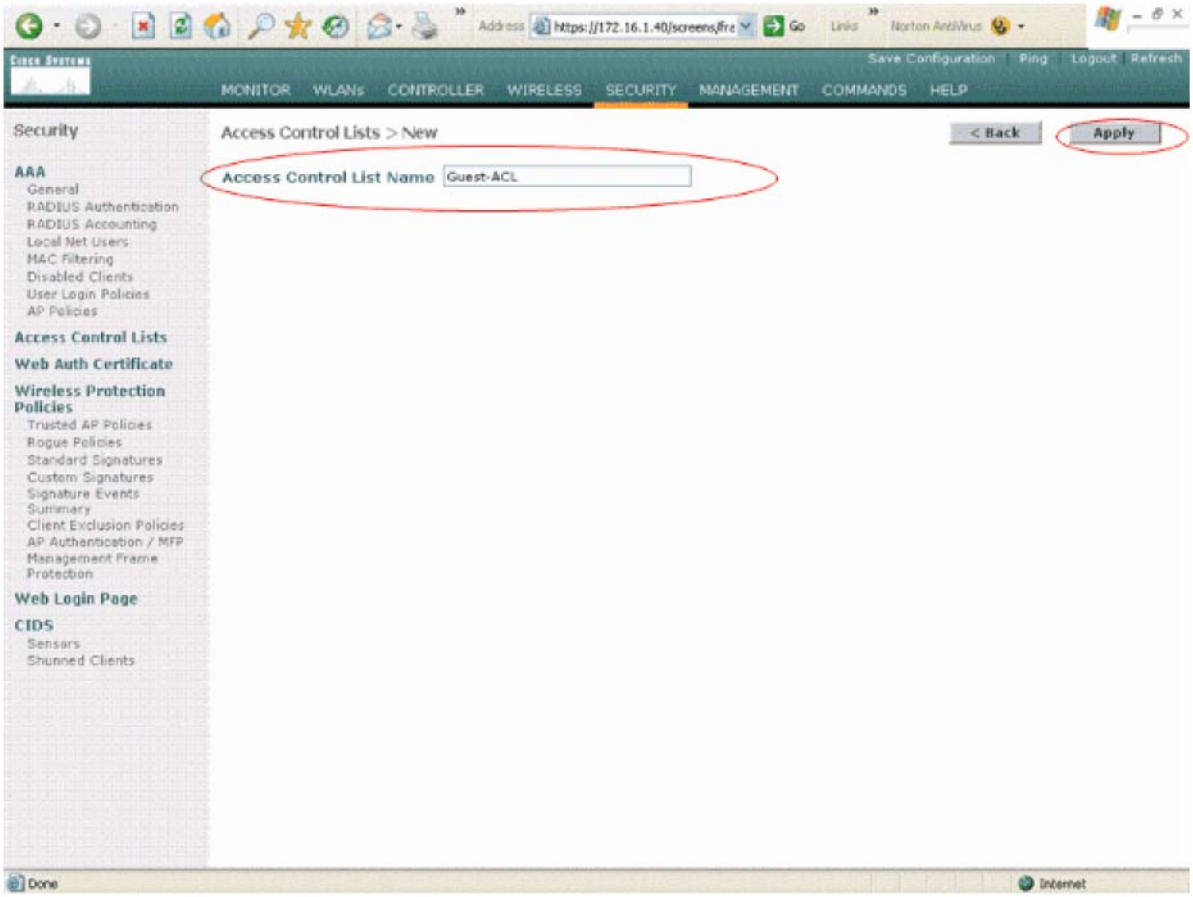
1. 进入无线控制器GUI，选择 **Security > Access Control Lists.**

   Access Control Lists的页面显示出来。这个页面上列出了在无线控制器上配置的ACL，你也可以编辑或删除任何一个ACL。创建一个新的ACL，点击 **New.**

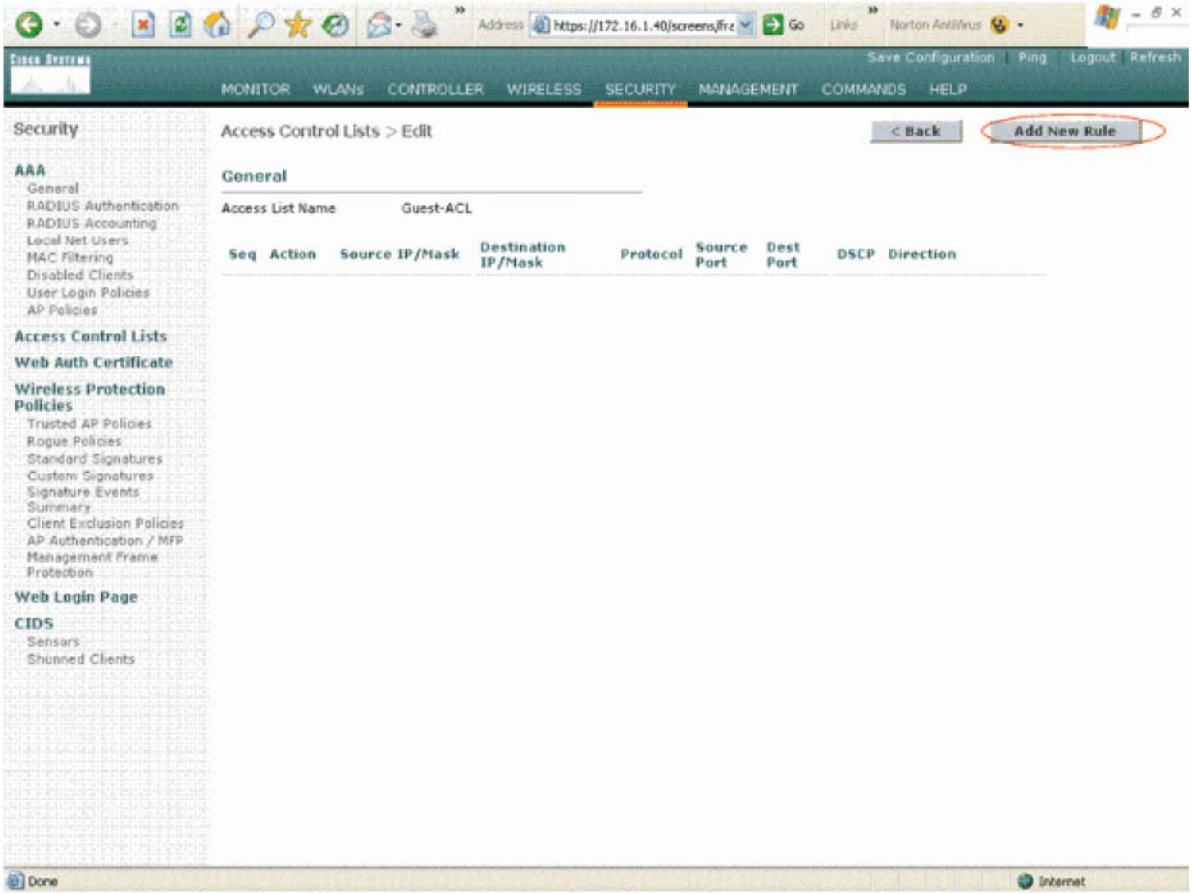


2. 输入ACL的命名，点击 **Apply.**

   你可以输入最多32个字母数字的字符。在这个例子中，ACL的命名是 **Guest-ACL.** ACL创建之后，点击 **Edit** 来为ACL创建规则。



3. 当 Access Control Lists > Edit 的页面显示出来，点击 **Add New Rule.** 则 Access Control Lists > Rules > New 的页面显示出来。



4. 配置允许访客用户访问如下服务的规则：

    - 无线客户端与DHCP服务器之间的DHCP数据
    - 网络中所有的设备之间的ICMP数据
    - 无线客户端与DNC服务器之间的DNS数据
    - Telnet服务到特定的子网

配置允许访客服务的规则

本章节举例说明如何为如下的服务配置规则：

- 无线客户端与DHCP服务器之间的DHCP数据
- 网络中所有的设备之间的ICMP数据
- 无线客户端与DNC服务器之间的DNS数据
- Telnet服务到特定的子网

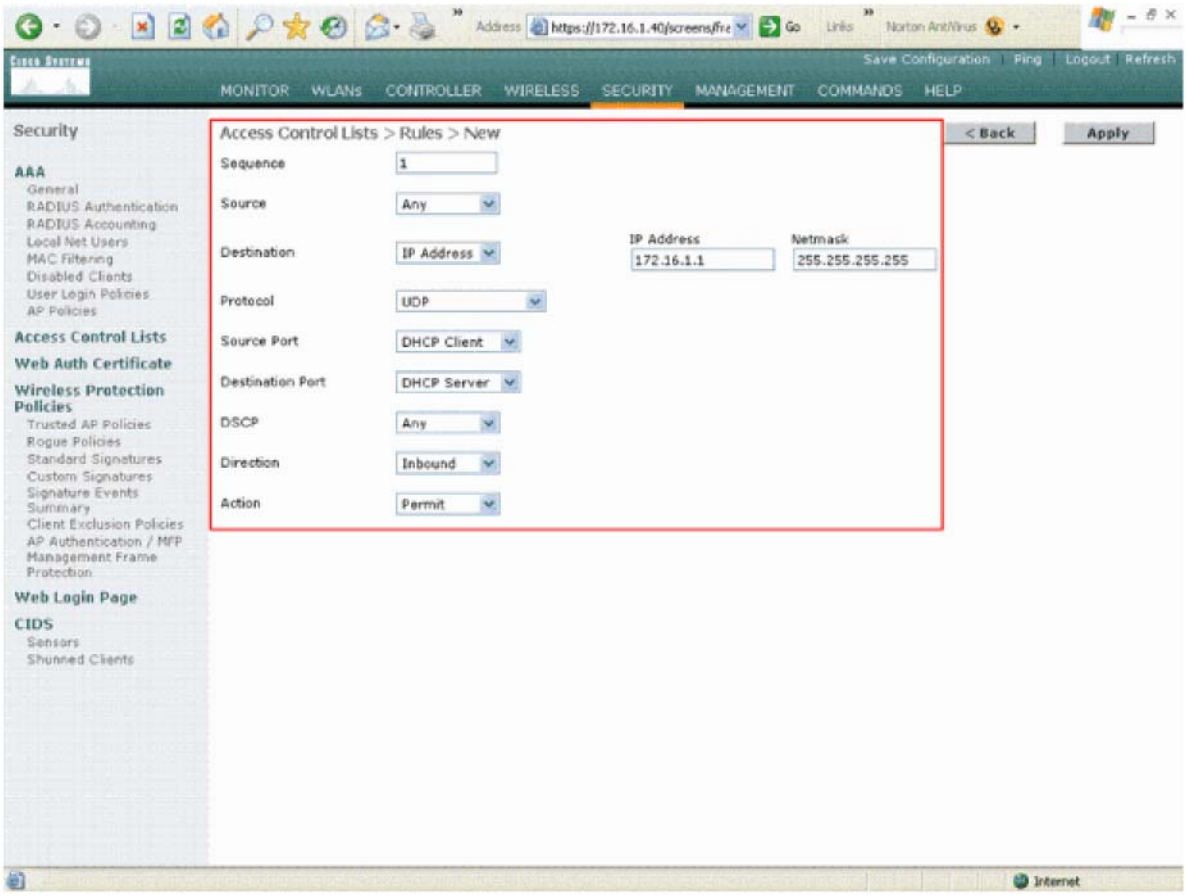
1. 为了配置DHCP服务的规则，选择源和目的的IP地址范围。

    在这个例子中源地址用 **any** ，表示任何无线客户端都可以访问到DHCP服务器。在这个例子中，服务器172.16.1.1作为DHCP和DNS服务器。因此，目的IP地址是172.16.1.1/255.255.255.255 (使用主机的掩码).

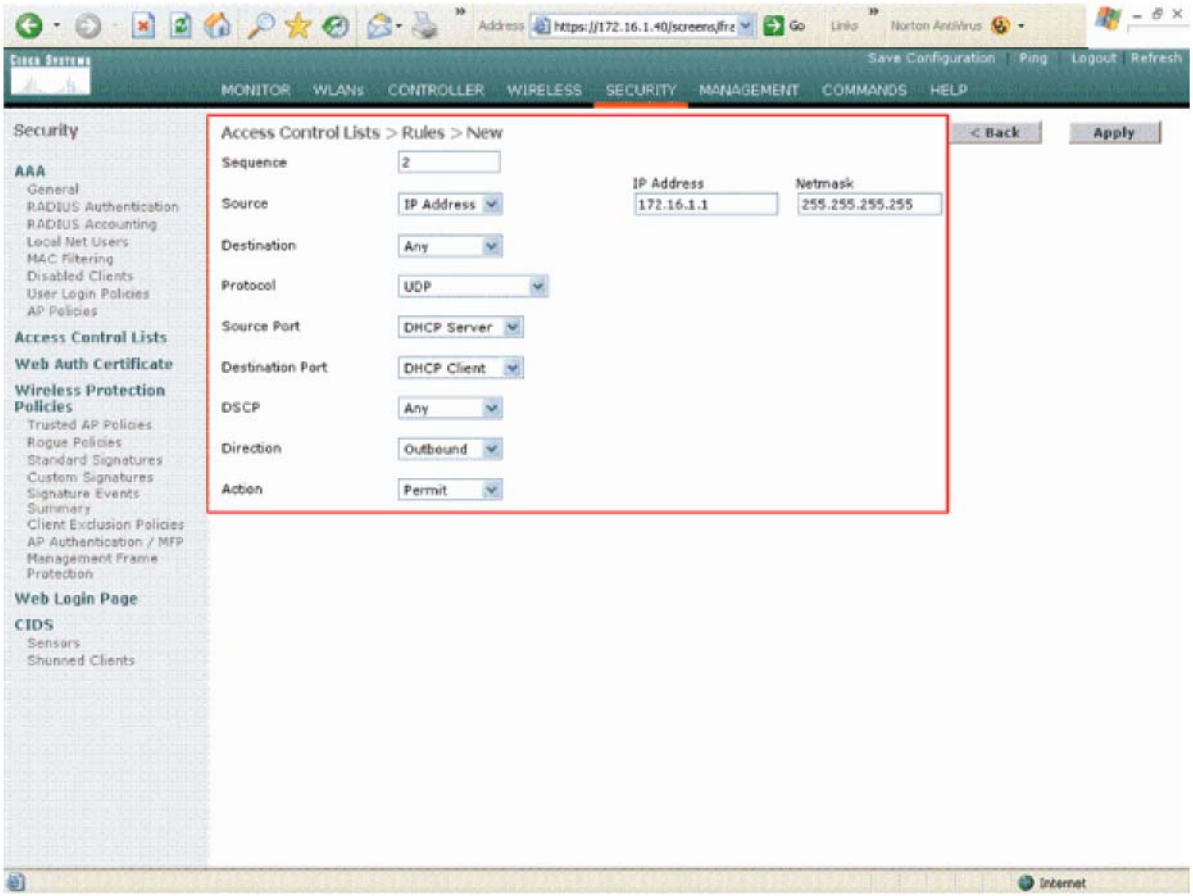
    Because DHCP is a UDP based protocol, 因为DHCP是基于UDP的协议，因此在Protocol的下拉菜单中选择 **UDP** 。如果你在前一步中选择TCP或UDP，2个附加的参数显示出来：源端口

和目的端口。指定源端口和目的端口。在这条规则中，源端口是 **DHCP Client** 而目的端口是 **DHCP Server.**

选择ACL应用的方向。因为这条规则是用于从客户端到服务器，这里选择 **Inbound.** 在Action的下拉菜单中，选择 **Permit** 使这个ACL允许从无线客户端到DHCP服务器的DHCP包。默认的参数是Deny。点击 **Apply.**



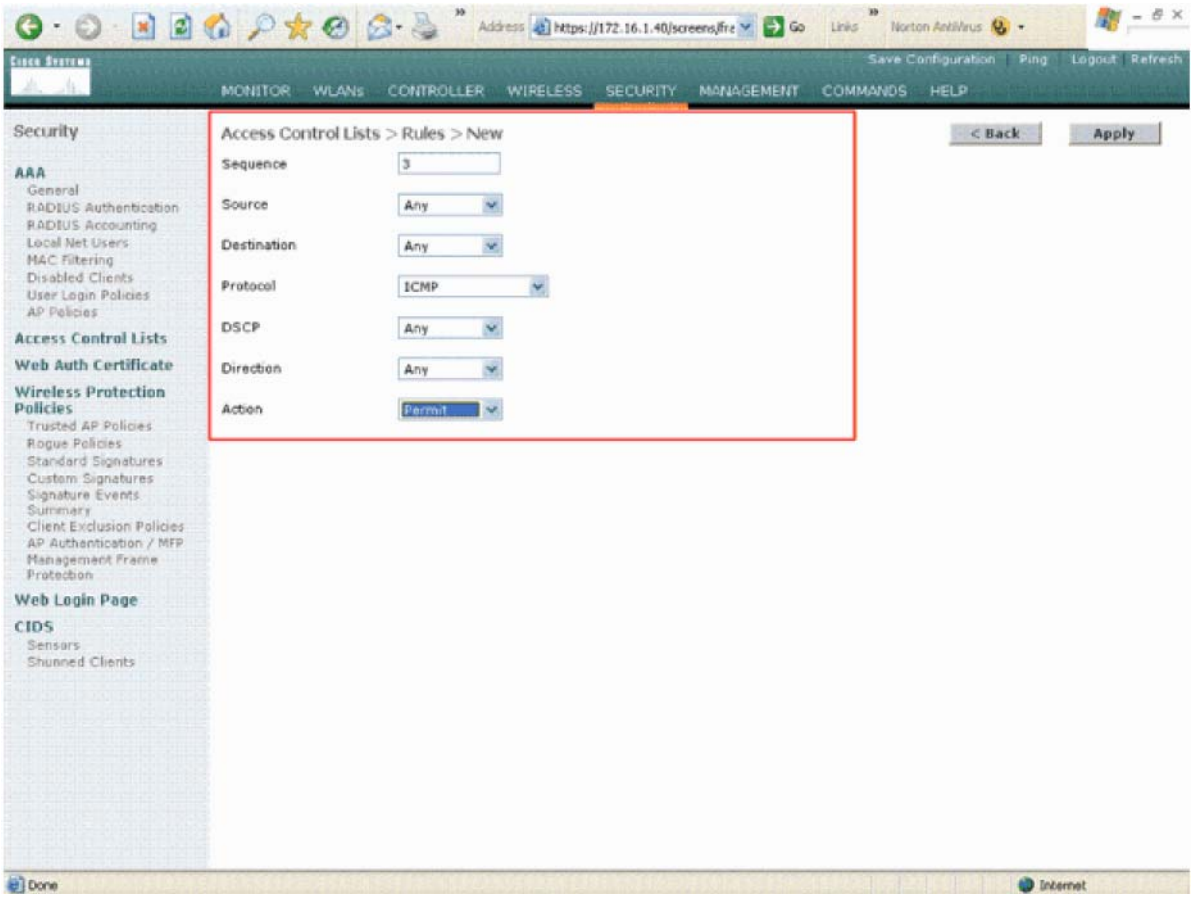
如果源或目的之一不是 **any,** 那么反方向的相反语句必须定义。如下是例子。



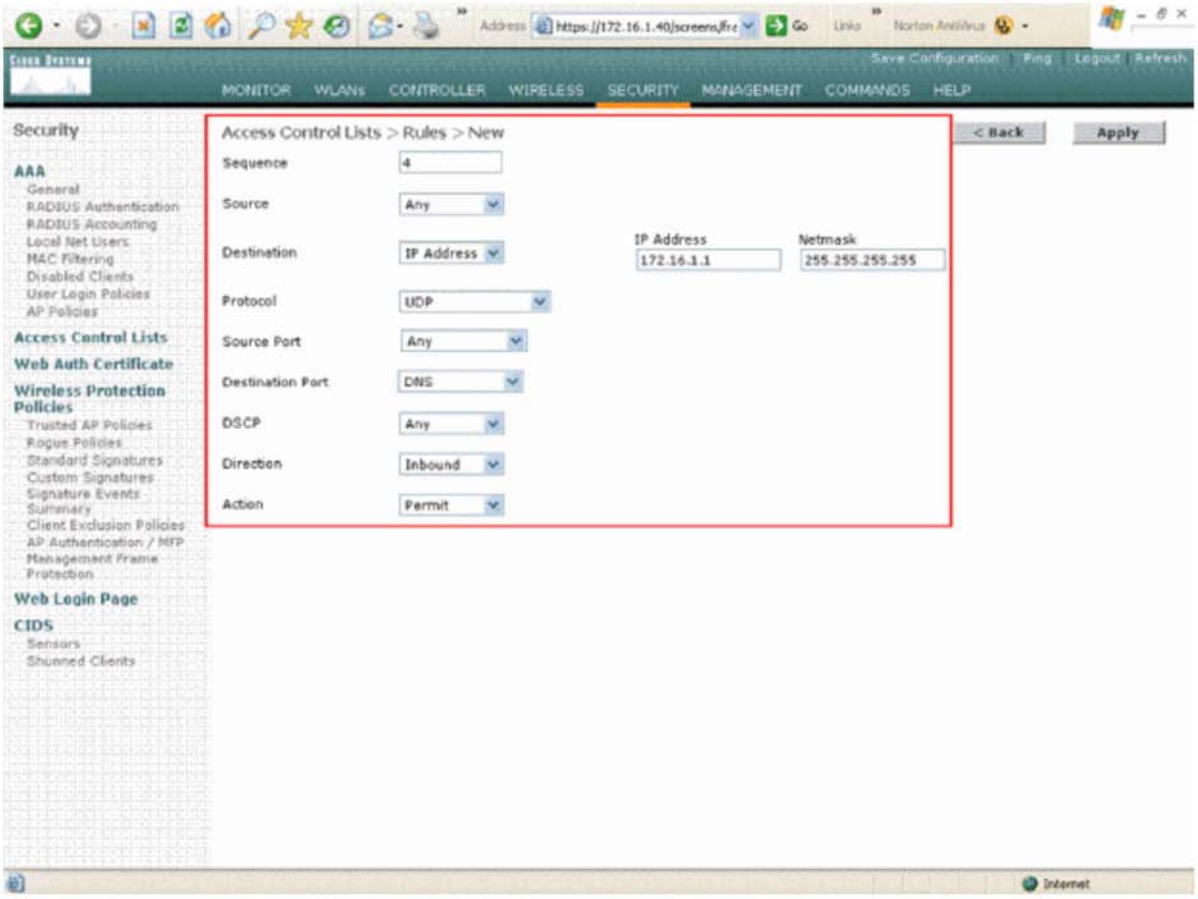
2. 为了定义允许所有设备之间的ICMP包的规则，在源和目的中选择 **any** ，这是默认的参数。

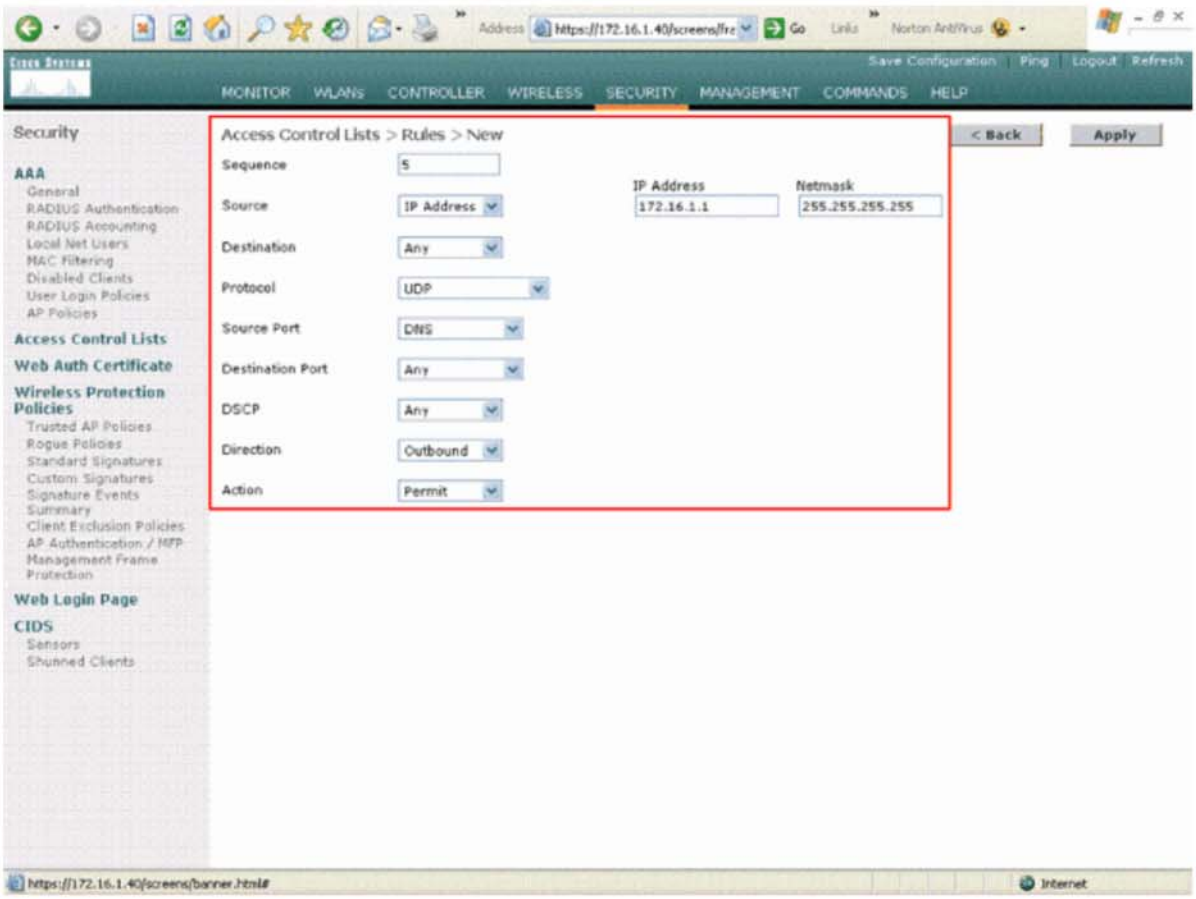
   在Protocol的下拉菜单中选择 **ICMP** 。因为这个例子中源和目的都选择了 **any** ，你可以不指定方向，可以用默认的参数 **any** 。并且，反方向的相反语句也不需要。

   在Action的下拉菜单中，选择 **Permit** 使这个ACL允许所有设备之间的ICMP数据包。点击**Apply.**

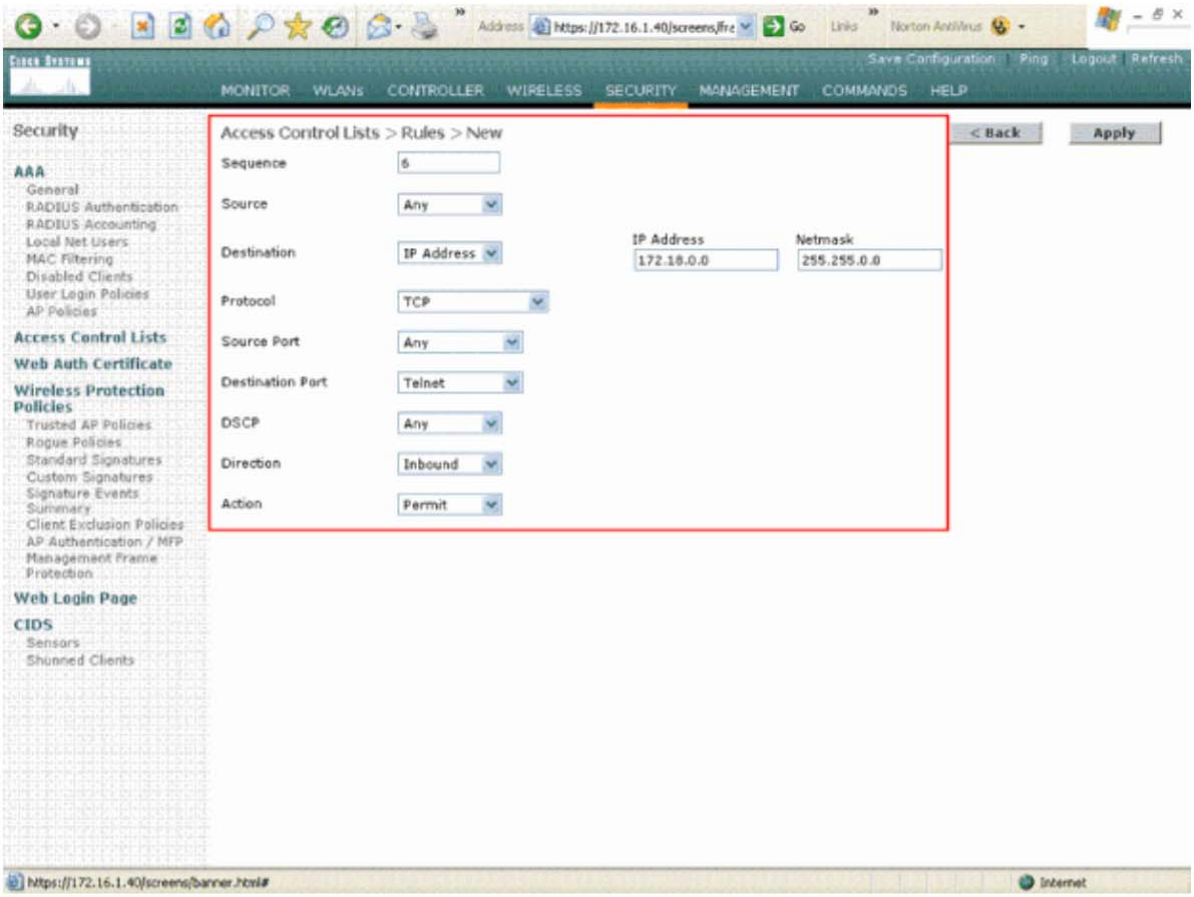


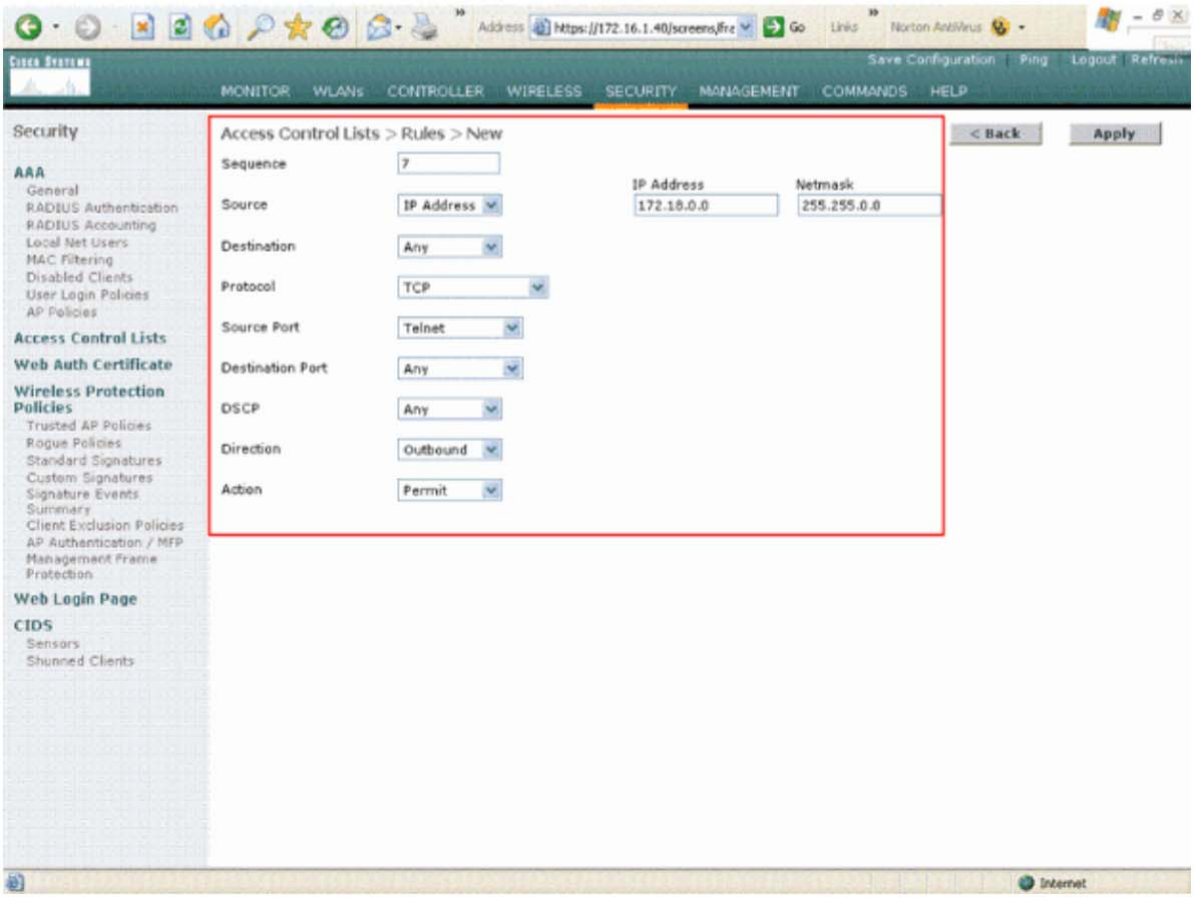
3. 类似的，为允许无线客户端的DNS服务和Telnet到特定的子网创建规则。如下是配置举例。



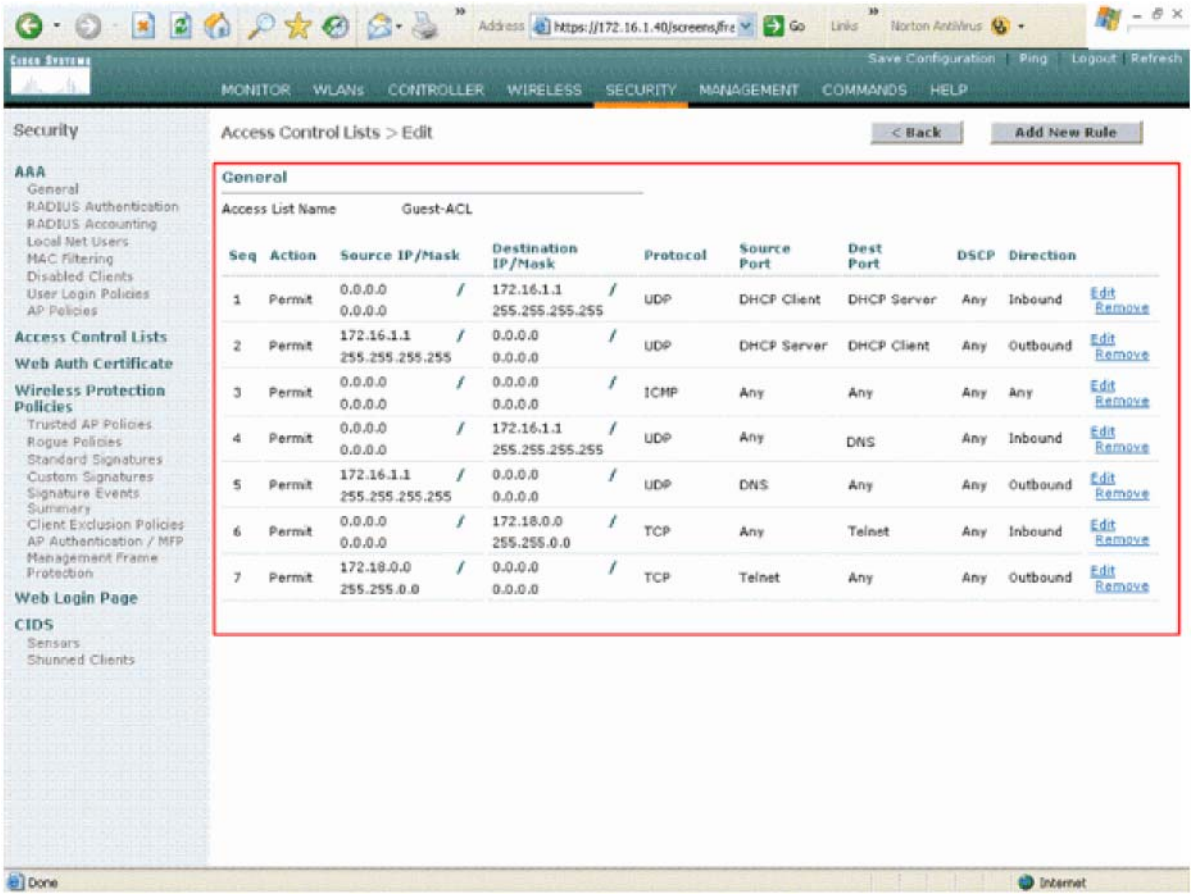


定义这条规则，允许无线客户端的Telnet服务。

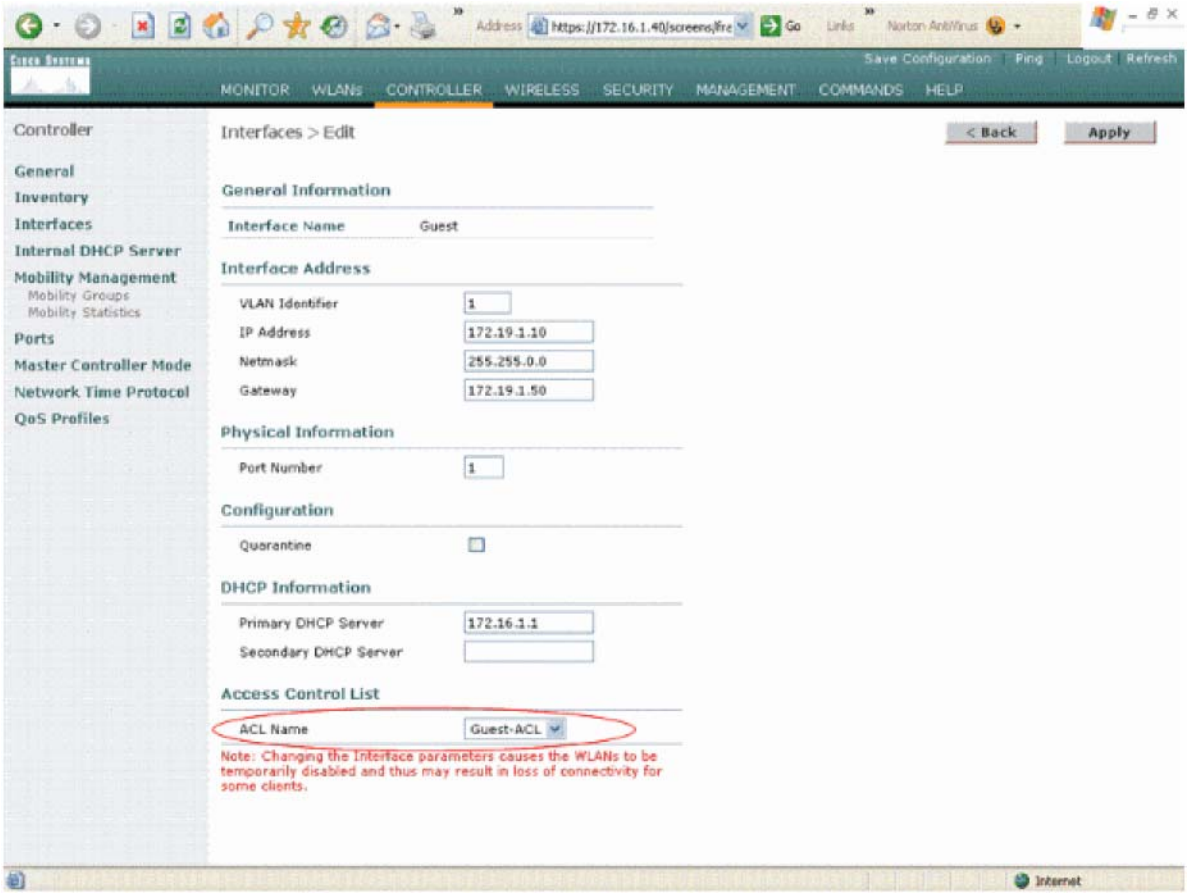




在 ACL > Edit 的页面上，列出了ACL中定义的所有规则。



4. ACL创建完成后，需要应用到动态的Interface上。为了应用ACL，选择 **Controller > Interfaces**，然后编辑想要应用ACL的Interface。
5. 在动态的Interface的 **Interfaces > Edit** 页面上，从ACL下拉菜单中选择适当的ACL。如下是配置举例。



这一步完成后，ACL就会允许或拒绝无线网络中使用这个动态的Interface的流量。

Note: 关于在无线控制器上如何用CLI来创建ACL的信息，参见Using the CLI to Configure Access Control Lists。

Note: 本文档中假定WLAN和动态Interface都已经配置好了。关于如何在无线控制器上配置动态Interface的信息，参见文档Wireless LAN Controllers Configuration Example的VLANs一节。

配置CPU的ACL

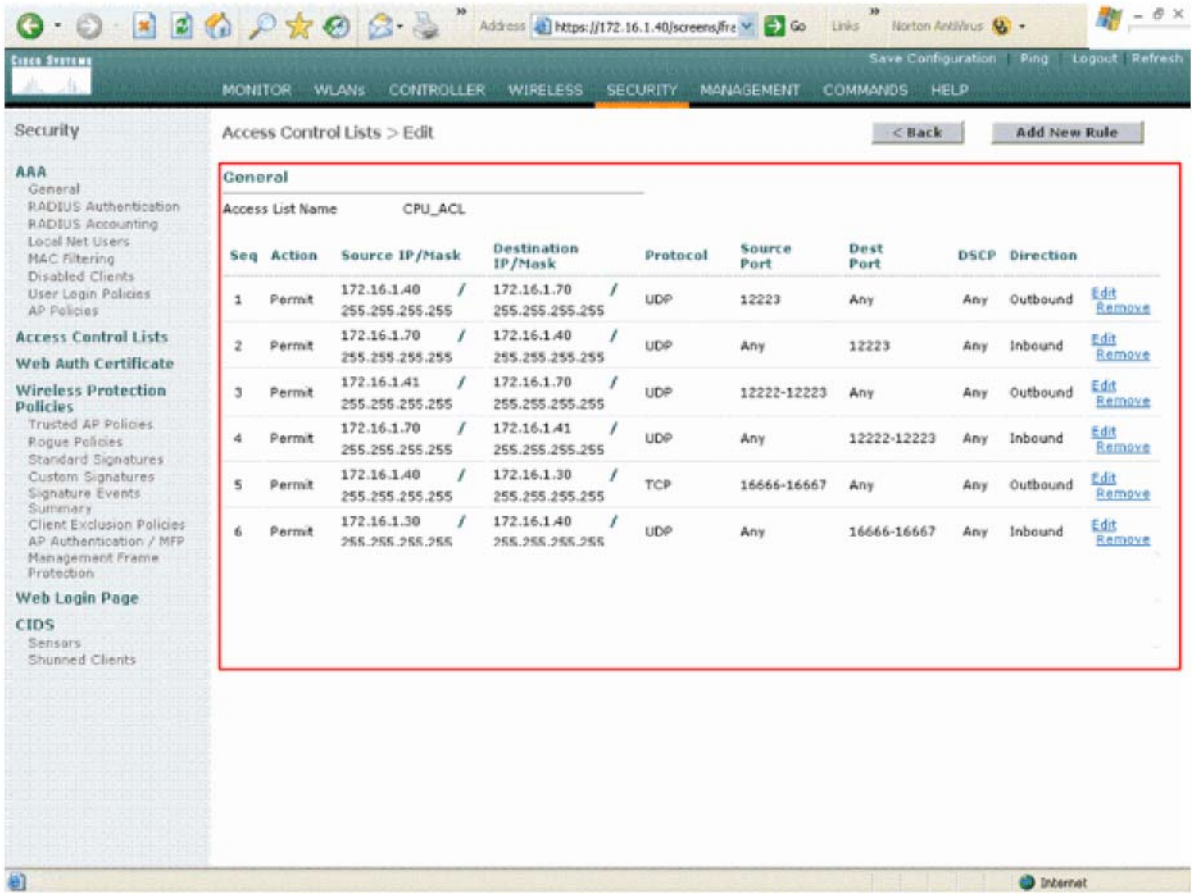
以前，无线控制器上的ACL无法过滤去往Management和AP Management端口的LWAPP数据流量，LWAPP控制流量和mobility流量。为了解决这个问题，过滤LWAPP和mobility流量，在无线控制器固件版本4.0中引进了CPU ACL。

配置CPU ACL包括2个步骤：

1. 为CPU ACL配置规则。
2. 在无线控制器上应用CPU ACL。

配置CPU ACL的规则的方法与其他的ACL类似。如下是一个CPU ACL的配置例子，允许控制器（Management Interface的IP地址是172.16.1.40，AP Management Interface的IP地址是172.16.1.41）和轻量级无线接入点（IP地址是172.16.1.70）之间的LWAPP数据和控制流量，其他的轻量级无线接入点的流量都被过滤掉。

这个例子中的CPU ACL同样允许Management Interface的IP地址是172.16.1.40的控制器和Management Interface的IP地址是172.16.1.30的控制器之间的mobility流量。



当CPU ACL创建完成后，你需要应用到无线控制器上。在无线控制器的CLI上输入如下命令，把CPU ACL应用到无线控制器上：

```
<Cisco Controller>config acl cpu <name of the ACL> <wired/wireless/both>
```

```
<Cisco Controller>config acl cpu CPU_ACL wired
```

输入如下命令禁用CPU ACL：

```
<Cisco Controller>config acl cpu none
```

Note: 这个例子中给出了如何配置只允许LWAPP和mobility流量的说明，当你在为ACL创建规则时，确保允许无线网络需要的所有协议，因为在每个ACL的最后有一条隐式的deny。

验证

思科推荐你用无线客户端测试一下ACL以确保你配置正确。如果不能正常运作，则在ACL的页面上检查ACL并且检查ACL是否应用到了控制器的Interface上。

你可以用如下的 **show** 命令来验证你的配置：

- **show acl summary** 使用 **show acl summary** 这条命令来列出在控制器上配置的ACL。

如下是举例：

```
(Cisco Controller) >show acl summary

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

- **show acl detailed *ACL_Name*** 列出ACL的具体信息。

如下是举例：

```
(Cisco Controller) >show acl detailed Guest-ACL
                  Source                          Destination                Source
I  Dir       IP Address/Netmask              IP Address/Netmask        Prot    Rang
-- --- ------------------------------ ------------------------------ ---- -------
 1  In          0.0.0.0/0.0.0.0              172.16.1.1/255.255.255.255   17    68-6
 2 Out       172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    67-6
 3 Any          0.0.0.0/0.0.0.0                 0.0.0.0/0.0.0.0            1     0-6
 4  In          0.0.0.0/0.0.0.0              172.16.1.1/255.255.255.255   17     0-6
 5 Out       172.16.1.1/255.255.255.255         0.0.0.0/0.0.0.0           17    53-5
 6  In          0.0.0.0/0.0.0.0              172.18.0.0/255.255.0.0             60-6
 7 Out       172.18.0.0/255.255.0.0             0.0.0.0/0.0.0.0            6    23-2
```

- **show acl cpu** 使用 **show acl cpu** 这条命令来列出CPU ACL。

如下是举例：

```
(Cisco Controller) >show acl cpu

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

排障

控制器固件版本4.2.61.0或更高版本中，可以配置ACL计数器。ACL计数器可以帮助确定哪个ACL应用到了通过控制器的数据包。这个特性在系统排障时非常有用。

ACL计数器在如下的控制器上有：

- 4400系列
- 思科WiSM
- Catalyst 3750G 集成无线控制器交换机

根据如下步骤起用这个特性：

1. 点击 **Security > Access Control Lists > Access Control Lists** 打开 Access Control Lists 页面。

   这个页面上列出在控制器上配置的所有的ACL。
2. 为了查看数据包有没有命中控制器上配置的ACL，选中 **Enable Counters** 并且点击 **Apply.** 在默认情况下是没有选中的。

3. 如果你要把ACL的计数器清零，把鼠标指针放在ACL的蓝色的下拉箭头上，选择 **Clear Counters.**

NetPro论坛 – 特殊的会话

Networking Professionals Connection是一个让网络专家们分享网络解决方案、产品和技术相关的问题、建议及信息的论坛。这些特殊的链接是一些在这个技术领域内最新的会话。

NetPro论坛 - 无线的特殊的会话

Wireless - Mobility: WLAN Radio Standards

Wireless - Mobility: Security and Network Management

Wireless - Mobility: Getting Started with Wireless

Wireless - Mobility: General

相关信息

- **VLANs on Wireless LAN Controllers Configuration Example**
- **Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)**
- **Cisco Wireless LAN Controller Configuration Guide, Release 4.0**
- **Wireless Support Page**
- **Technical Support & Documentation - Cisco Systems**

更新: Jan 21, 2008 文档 ID: 71978