ACLs on Wireless LAN Controller Configuration Example

Document ID: 71978

Introduction

This document explains how to configure access control lists (ACLs) on Wireless LAN Controllers (WLCs) to filter traffic that enters and leaves a WLAN.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure the WLC and Lightweight Access Point (LAP) for basic operation
- Basic knowledge of Lightweight Access Point Protocol (LWAPP) and wireless security methods

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2000 Series WLC that runs firmware 4.0
- Cisco 1000 Series LAP
- Cisco 802.11a/b/g Wireless client adapter that runs firmware 2.6
- Cisco Aironet Desktop Utility (ADU) version 2.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

ACLs on WLCs

ACLs on the WLC are meant to restrict or permit wireless clients to services on its WLAN.

Before WLC firmware version 4.0, ACLs are bypassed on the Management Interface, so you cannot affect traffic destined to the WLC other than preventing wireless clients from managing the controller with the **Management Via Wireless** option. Therefore, ACLs can only be applied to dynamic interfaces. In WLC firmware version 4.0, there are CPU ACLs which can filter traffic destined for the Management Interface. An example of how to configure CPU ACLs is provided later in this document.

You can define up to 64 ACLs, each with up to 64 rules (or filters). Each rule has parameters that affect its action. When a packet matches all of the parameters for a rule, the action set for that rule is applied to the packet. You can configure ACLs through either the GUI or the CLI.

These are some of the rules you need to understand before you configure an ACL on the WLC:

- If the source *and* destination are **any**, the direction in which this ACL is applied can be **any**.
- If either the source *or* destination are **not any**, then the direction of the filter must be specified, and an inverse statement in the opposite direction must be created.
- The WLC's notion of inbound versus outbound is nonintuitive. It is from the perspective of the WLC facing towards the wireless client, rather than from the perspective of the client. So, inbound direction means a packet that comes into the WLC from the wireless client and outbound direction means a packet that exits from the WLC towards the wireless client.
- There is an implicit deny at the end of the ACL.

Considerations When Configuring ACLs in WLCs

ALCs in WLCs work differently than in routers. These are a few things to remember when you configure ACLs in WLCs:

- The most common mistake is to select IP when you intend to deny or allow IP packets. Because you select what is inside the IP packet, you end up denying or allowing IP−in−IP packets.
- Controller ACLs cannot block 1.1.1.1 (virtual IP address), and hence DHCP packets for wireless clients.
- Controller ACLs cannot block multicast and broadcast packets because they are forwarded out the management interface to the access points (APs).
- Unlike a router, the ACL controls traffic in both directions when applied to an interface, but it does not perform stateful firewalling. If you forget to open a hole in the ACL for returning traffic, this causes a problem.
- Controller ACLs only block IP packets. You cannot block Layer 2 ACLs or Layer 3 packets that are not IP.
- Controller ACLs do not use inverse masks like the routers. Here, 255 means match that octet of the IP address exactly.
- ACLs on the controller are done in software and impact forwarding performance.

Configure ACL on WLCs

This section describes how to configure an ACL on the WLC. The objective is to configure an ACL that allows guest clients to access these services:

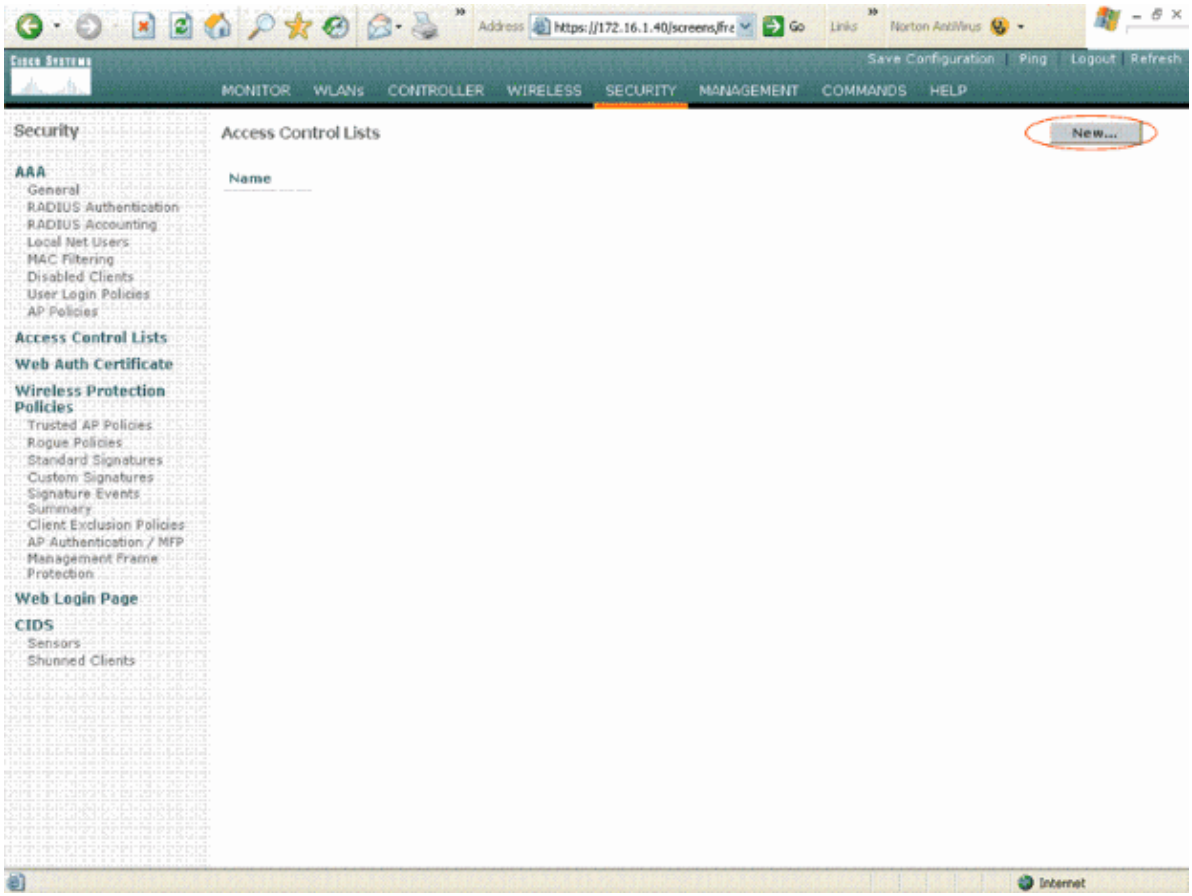
- Dynamic Host Configuration Protocol (DHCP) between the wireless clients and DHCP server
- Internet Control Message Protocol (ICMP) between all devices in the network

- Domain Name System (DNS) between the wireless clients and the DNS server
- Telnet to a specific subnet

All other services must be blocked for the wireless clients. Complete these steps in order to create the ACL using the WLC GUI:

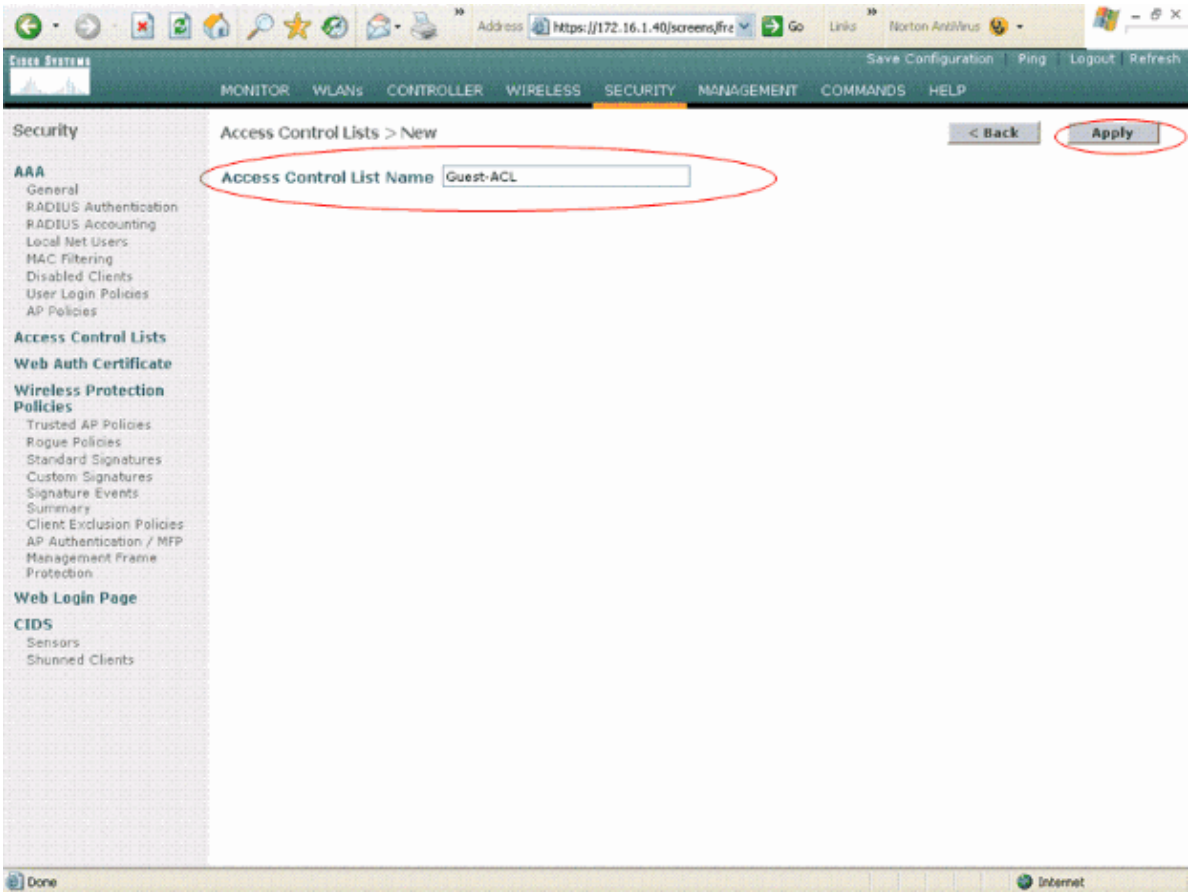
1. Go to the WLC GUI and choose **Security > Access Control Lists**.

   The Access Control Lists page appears. This page lists the ACLs that are configured on the WLC. It also enables you to edit or remove any of the ACLs. In order to create a new ACL, click **New**.



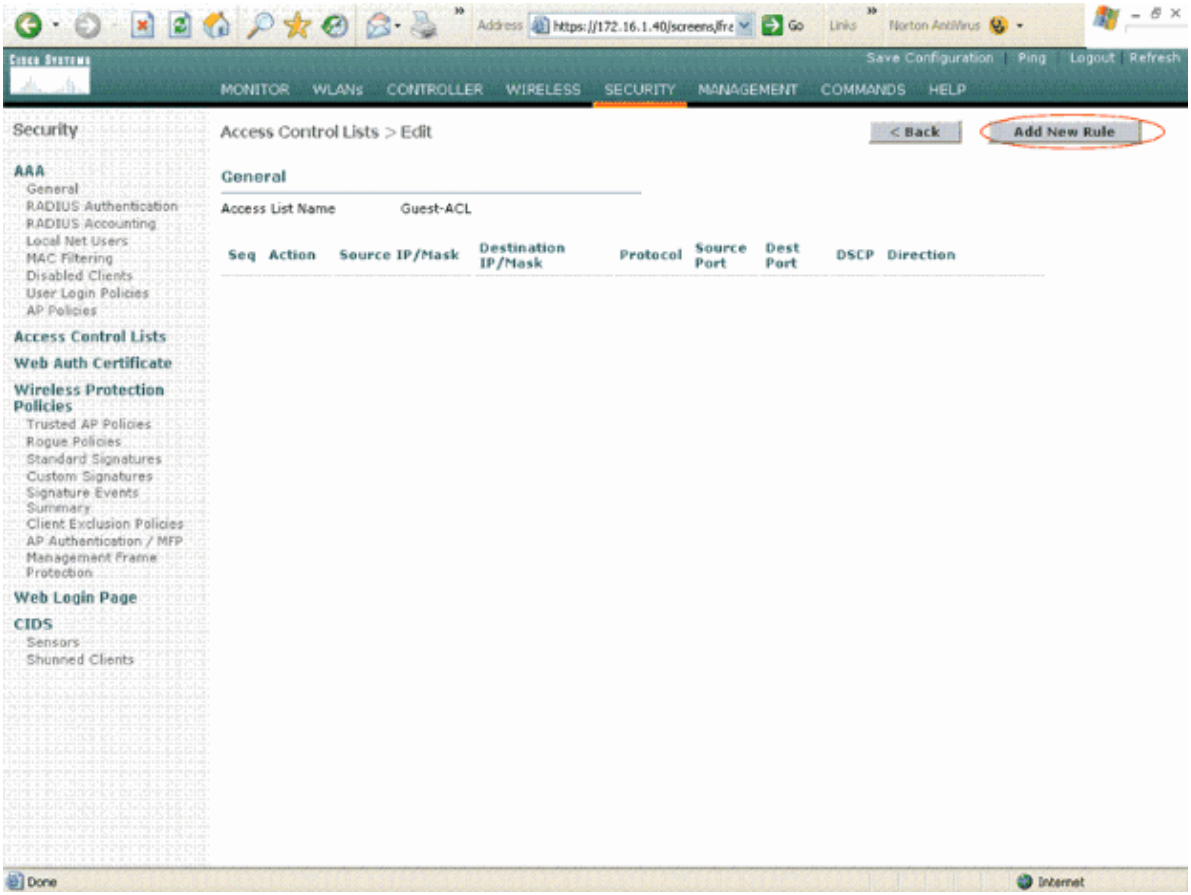
2. Enter the name of the ACL and click **Apply**.

   You can enter up to 32 alphanumeric characters. In this example, the name of the ACL is **Guest−ACL**. Once the ACL is created, click **Edit** in order to create rules for the ACL.



3. When the Access Control Lists > Edit page appears, click **Add New Rule**.

   The Access Control Lists > Rules > New page appears.



4. Configure rules that allow a guest user these services:

    - ♦ DHCP between the wireless clients and DHCP server
    - ♦ ICMP between all devices in the network
    - ♦ DNS between the wireless clients and the DNS server
    - ♦ Telnet to a specific subnet

Configure Rules that Allow Guest User Services

This section shows an example for how to configure the rules for these services:

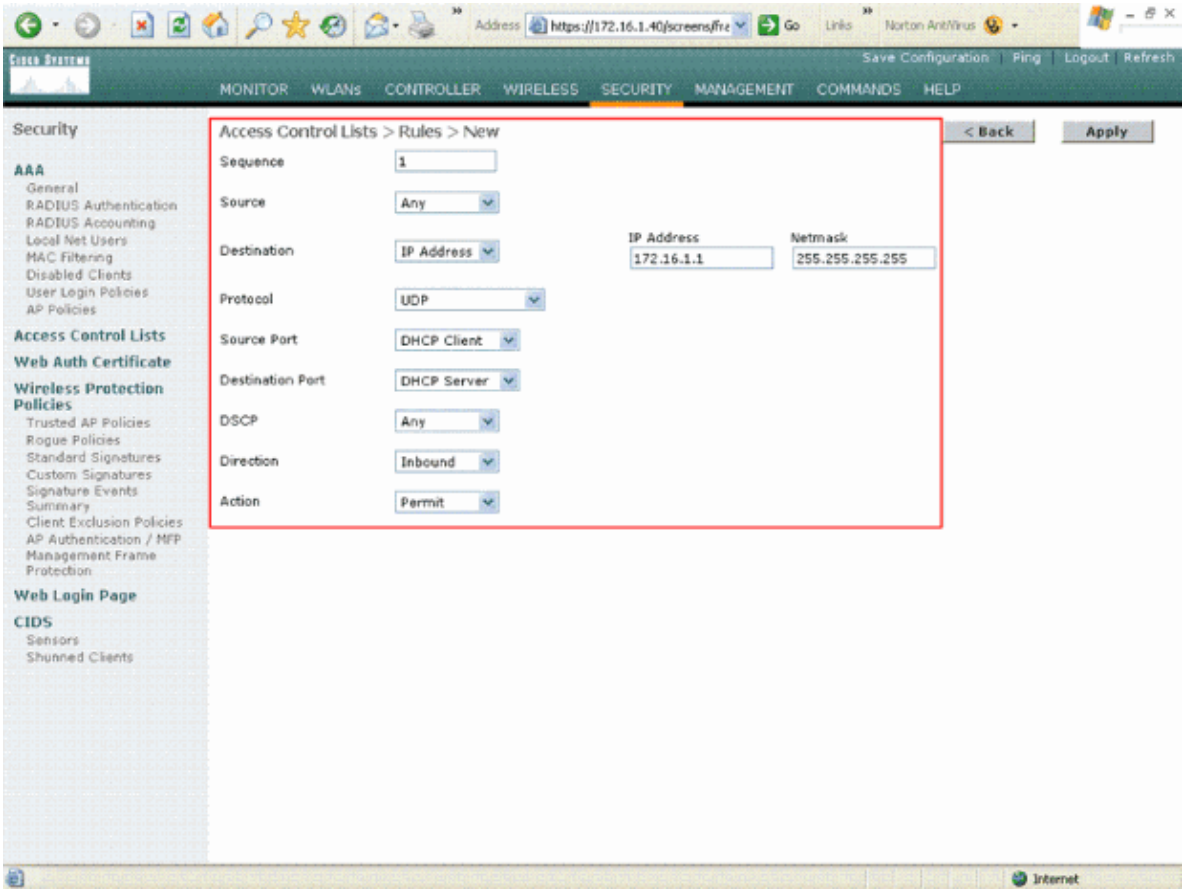
- DHCP between the wireless clients and DHCP server
- ICMP between all devices in the network
- DNS between the wireless clients and the DNS server
- Telnet to a specific subnet

1. In order to define the rule for DHCP service, select the source and destination IP ranges.

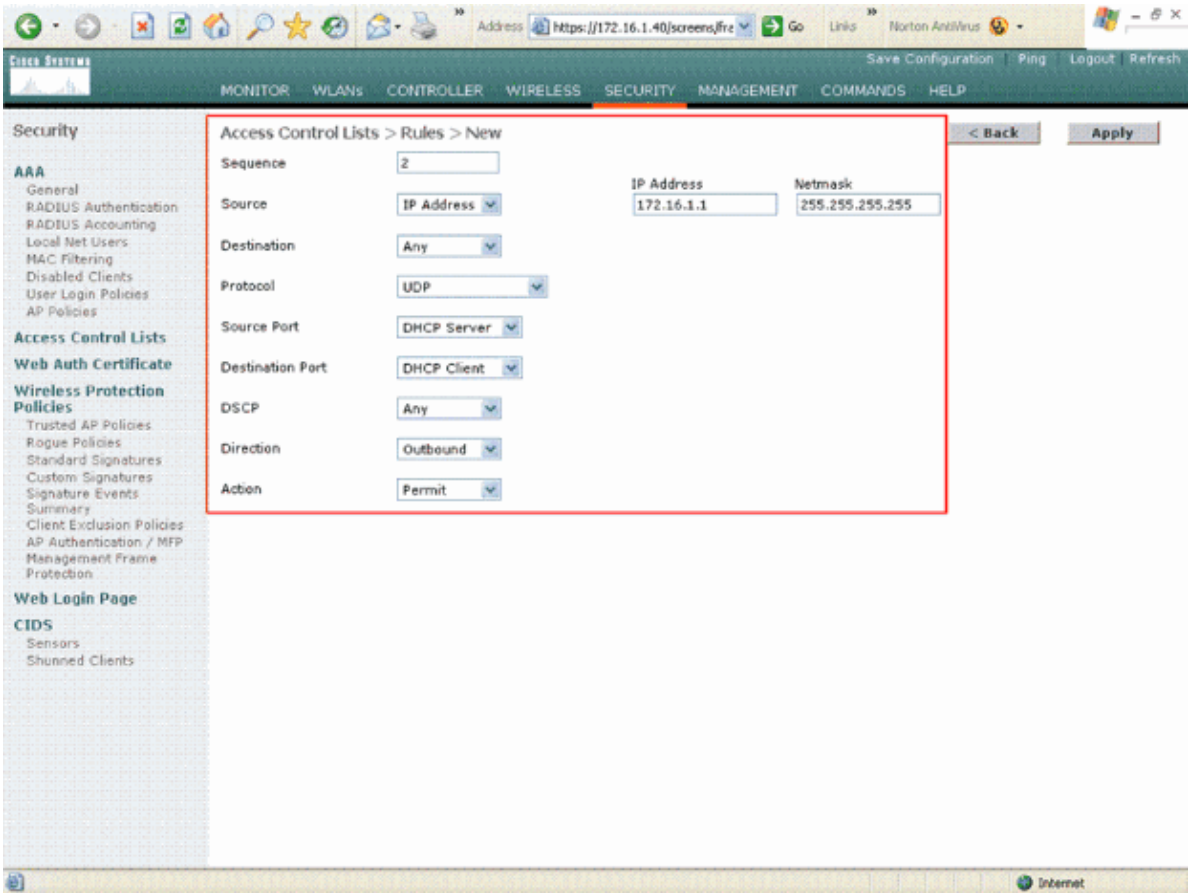
   This example uses **any** for the source which means that any wireless client is allowed access to the DHCP server. In this example, the server 172.16.1.1 acts as the DHCP and DNS server. So, the destination IP address is 172.16.1.1/255.255.255.255 (with a host mask).

   Because DHCP is a UDP based protocol, select **UDP** from the Protocol drop−down field. If you chose TCP or UDP in the previous step, two additional parameters appear: Source Port and Destination Port. Specify the Source and Destination port details. For this rule, the Source Port is **DHCP Client** and the Destination Port is **DHCP Server**.

   Choose the Direction in which the ACL is to be applied. Because this rule is from the client to the server, this example uses **Inbound**. From the Action drop−down box, choose **Permit** to cause this ACL to allow DHCP packets from the wireless client to the DHCP server. The default value is Deny. Click **Apply**.



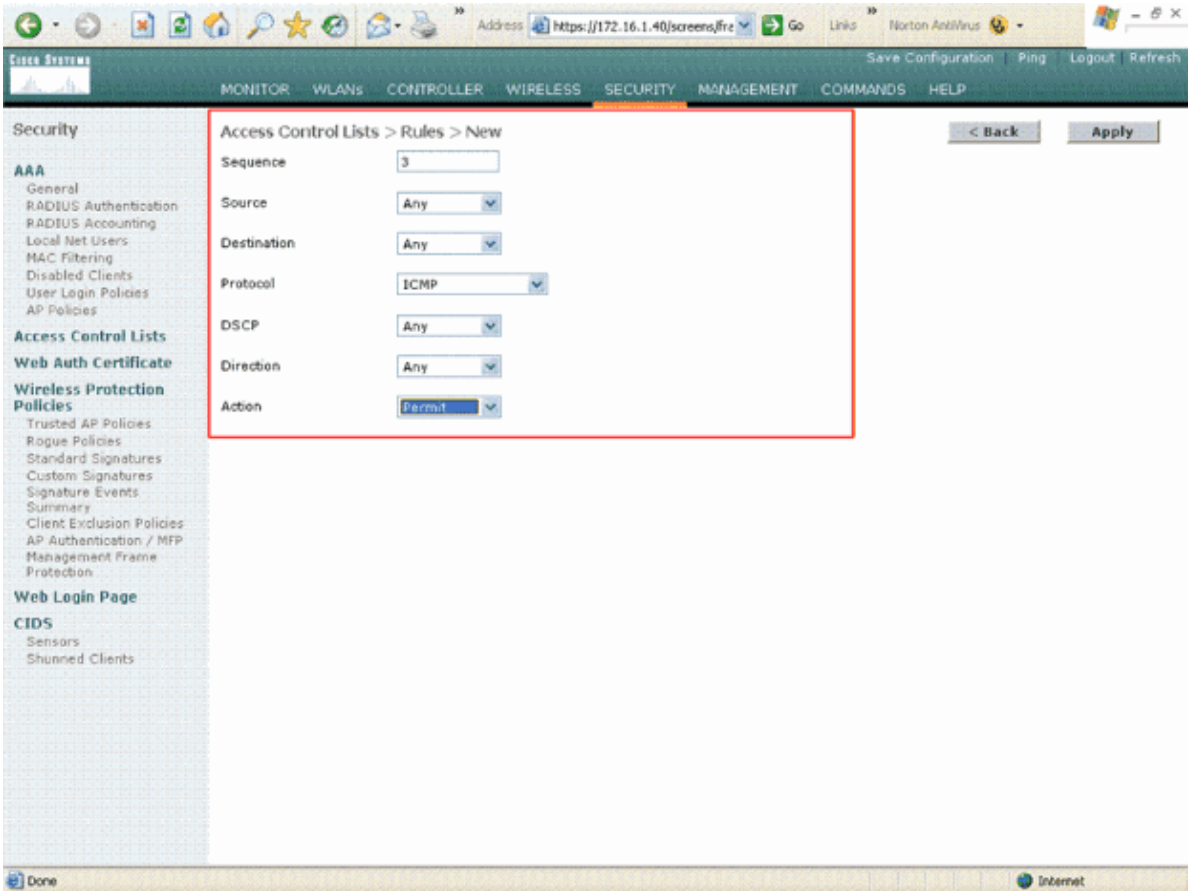
If either the source or destination are not **any**, then an inverse statement in the opposite direction must be created. Here is an example.



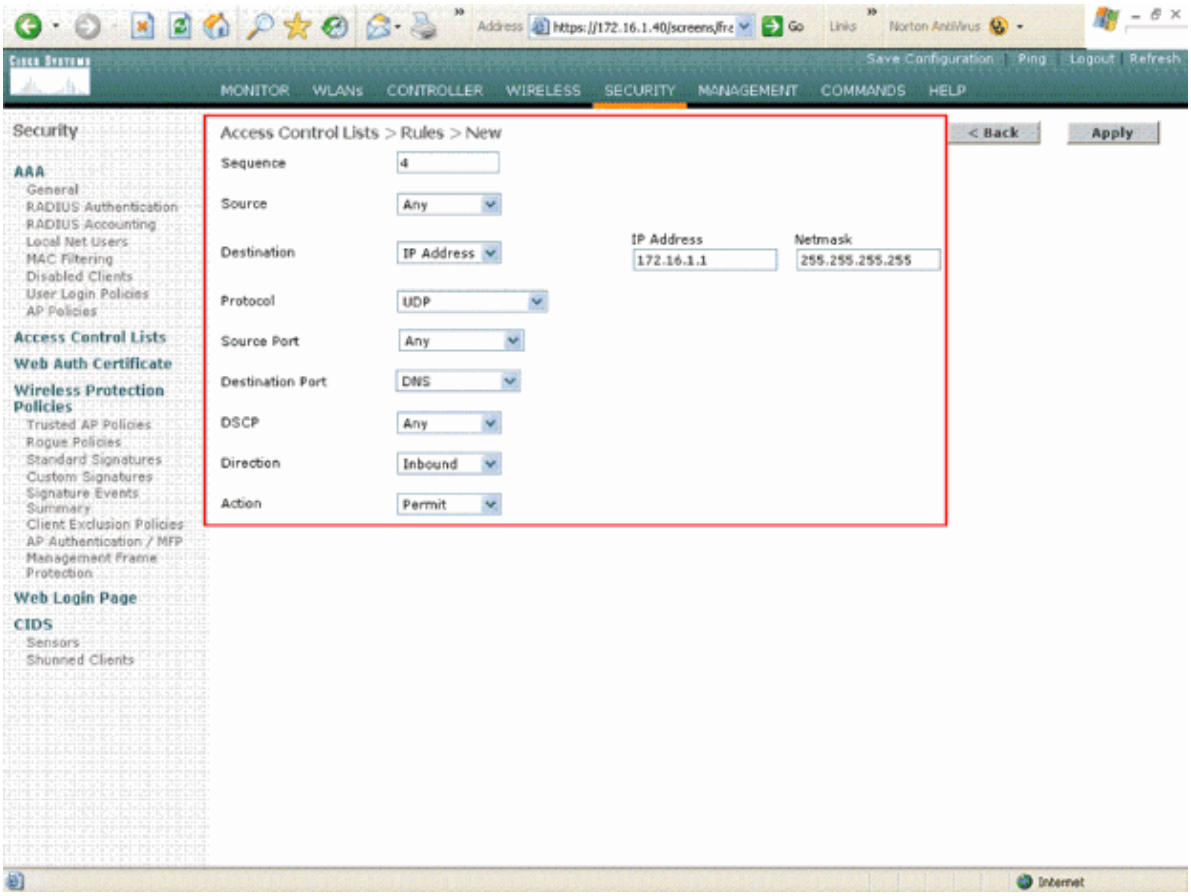
2. In order to define a rule that allows ICMP packets between all devices, select **any** for the Source and Destination fields. This is the default value.

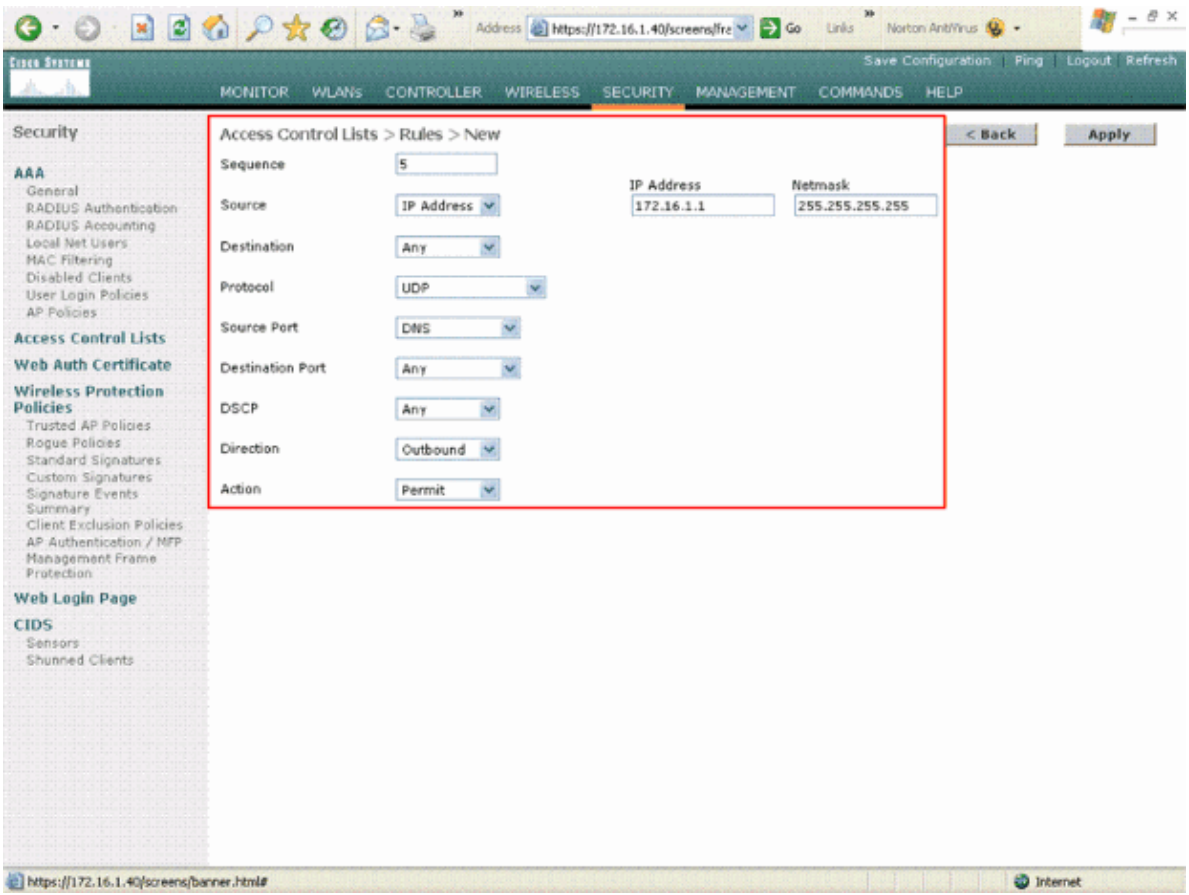
   Choose **ICMP** from the Protocol drop−down field. Because this example uses **any** for the Source and Destination fields, you do not have to specify the direction. It can be left at its default value of **any**. Also, the inverse statement in the opposite direction is not required.

   From the Action drop−down menu, choose **Permit** in order to cause this ACL to allow DHCP packets from the DHCP server to the wireless client. Click **Apply**.

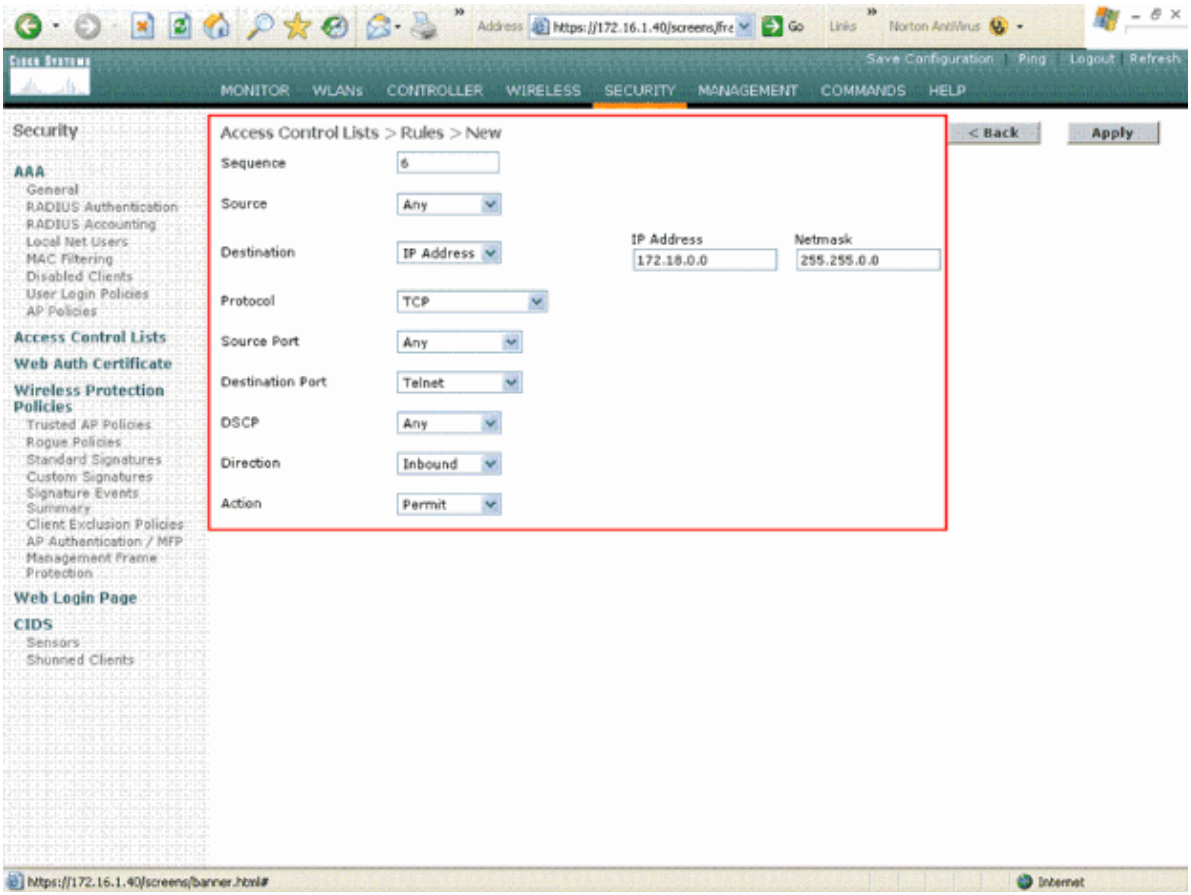


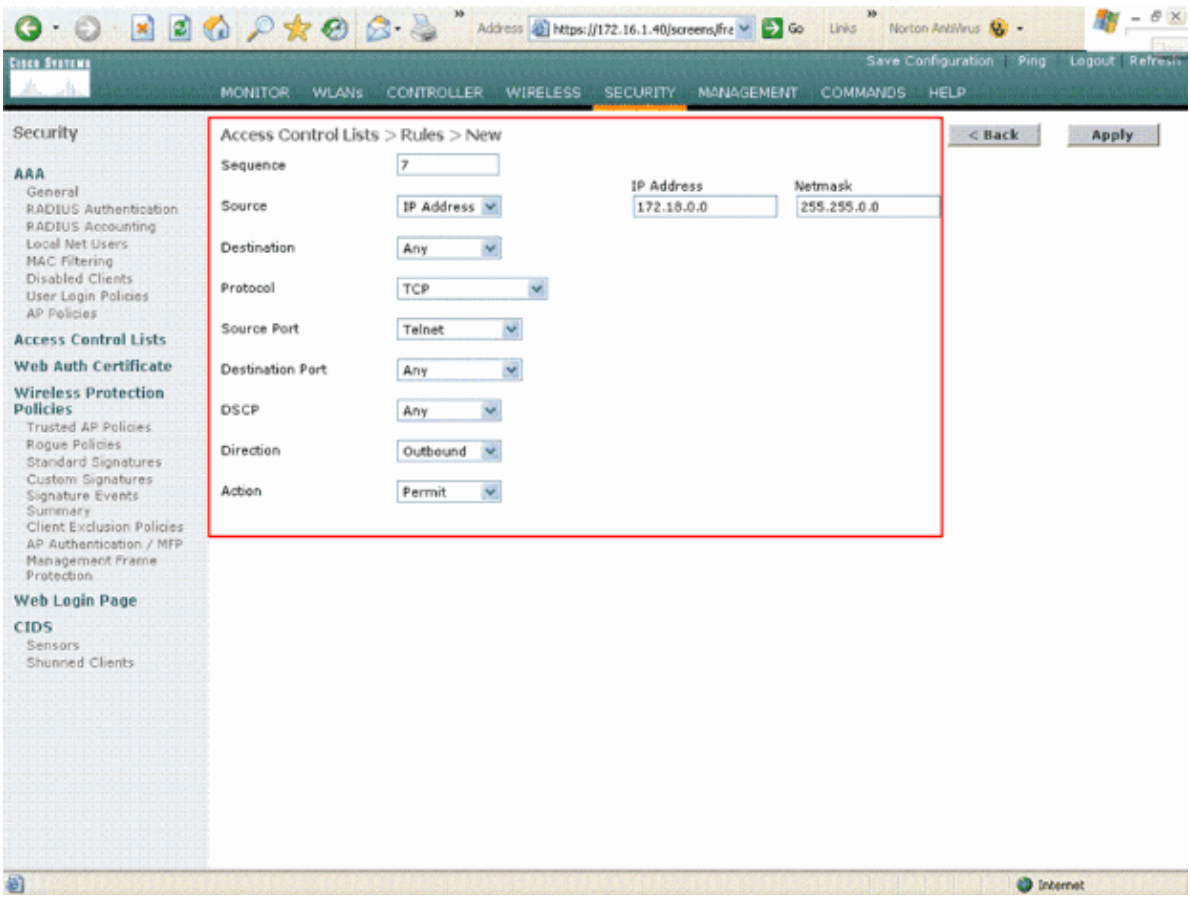
3. Similarly, create rules that allow DNS server access to all wireless clients and Telnet server access for the wireless client to a specific subnet. Here are the examples.



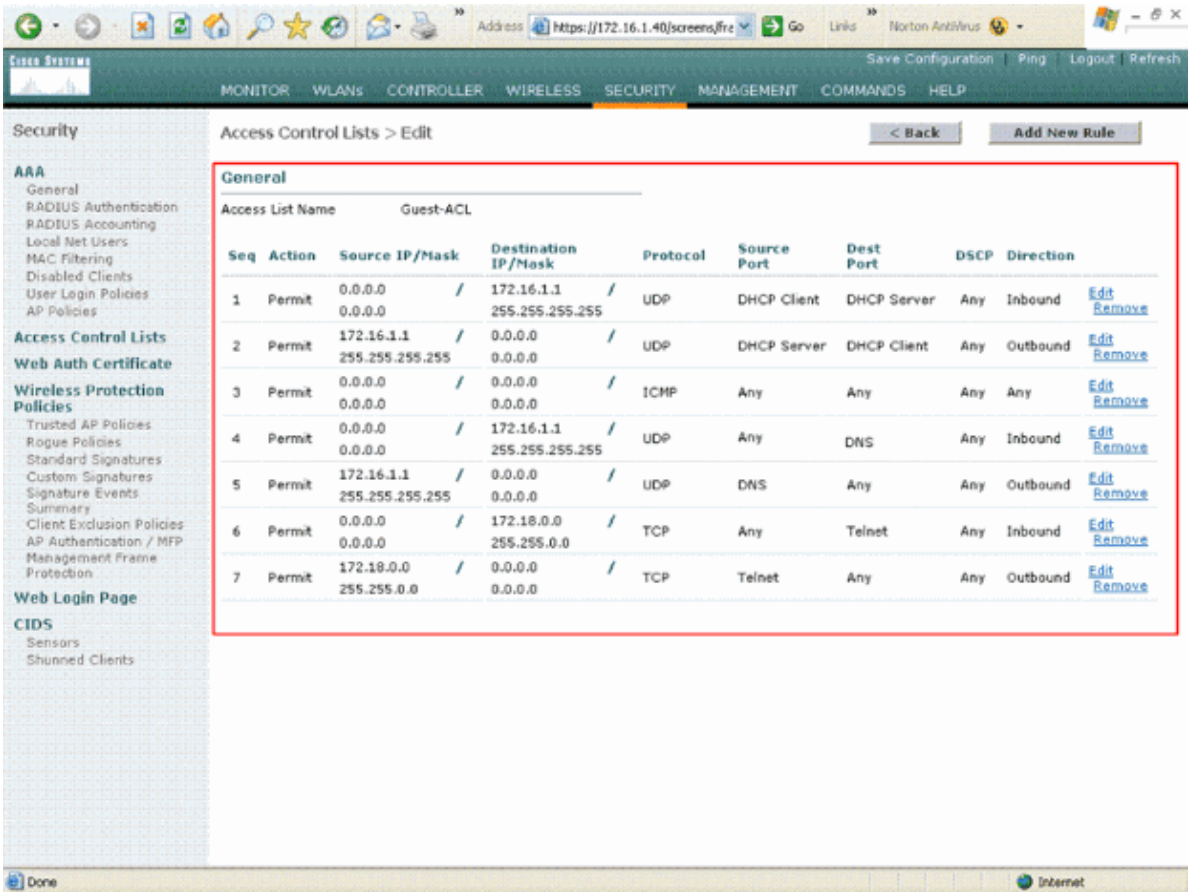


Define this rule in order to allow access for the wireless client to the Telnet service.

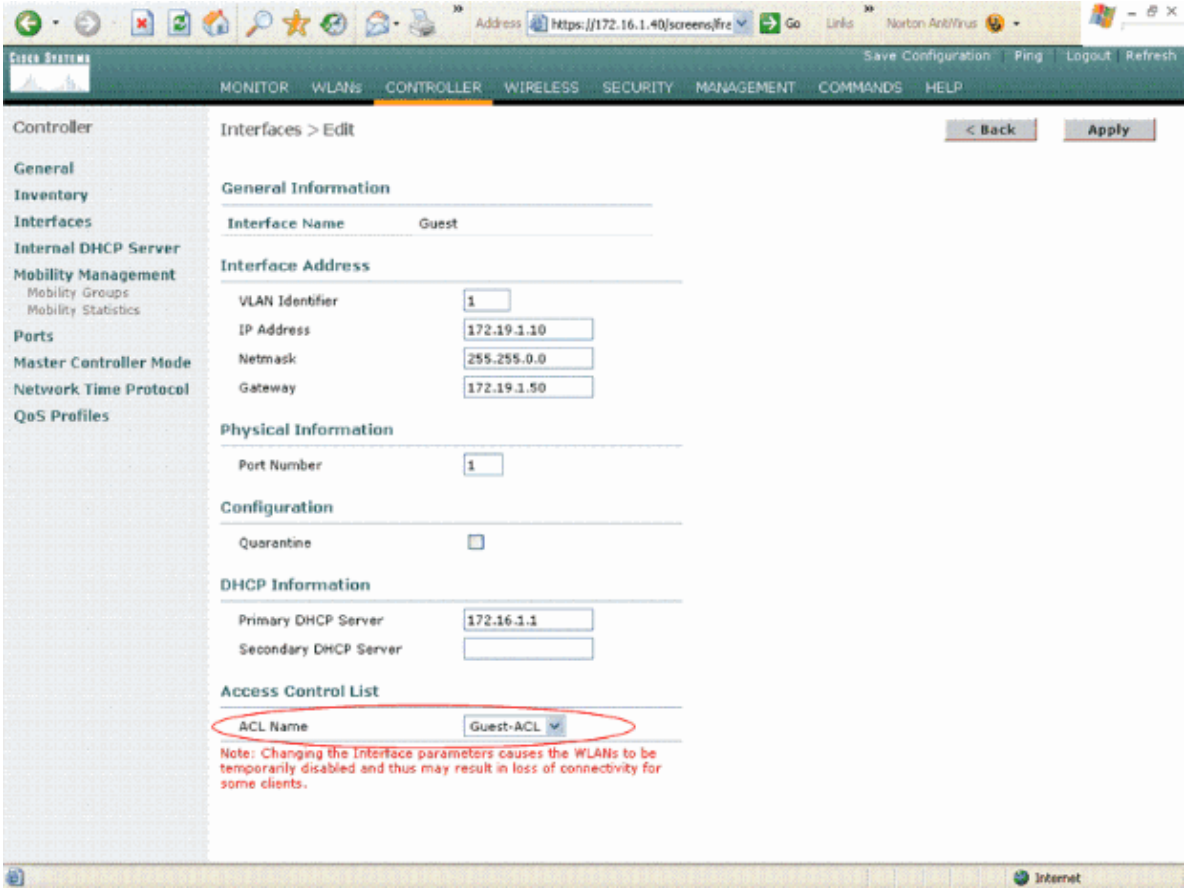




The ACL > Edit page lists all the rules that are defined for the ACL.



4. Once the ACL is created, it needs to be applied to a dynamic interface. In order to apply the ACL, choose **Controller > Interfaces** and edit the interface to which you want to apply the ACL.
5. In the **Interfaces > Edit** page for the dynamic interface, choose the appropriate ACL from the Access Control Lists drop−down menu. Here is an example.



Once this is done, the ACL permits and denies traffic (based on the configured rules) on the WLAN which uses this dynamic interface.

Note: Refer to Using the CLI to Configure Access Control Lists for information on how to create an ACL using the CLI on the WLC.

Note: This document assumes that WLANs and dynamic interfaces are configured. Refer to VLANs on Wireless LAN Controllers Configuration Example for information on how to create dynamic interfaces on WLCs.

Configure CPU ACLs

Previously, ACLs on WLCs did not have an option to filter LWAPP data traffic, LWAPP control traffic, and mobility traffic destined to the Management and AP Manager interfaces. In order to address this issue and filter LWAPP and mobility traffic, CPU ACLs were introduced with WLC firmware release 4.0.

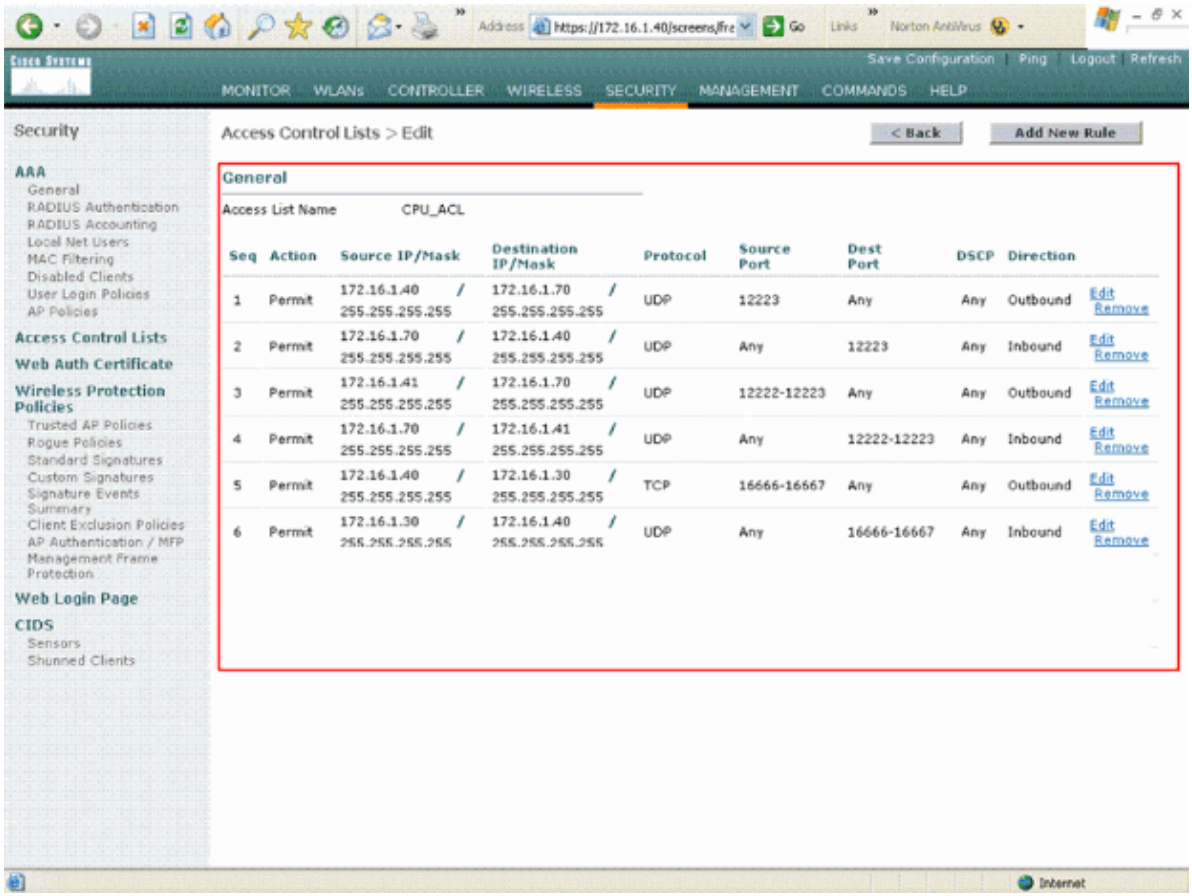
The configuration of CPU ACLs involves two steps:

1. Configure rules for the CPU ACL.
2. Apply the CPU ACL on the WLC.

The rules for the CPU ACL should be configured in a similar way to the other ACLs. Here is an example CPU ACL that allows LWAPP data and control traffic between the controller (with Management Interface IP address 172.16.1.40 and AP Manager Interface IP address 172.16.1.41) and the LAP (with IP address 172.16.1.70). Traffic from all other LAPs is filtered.

This example CPU ACL also allows mobility traffic between the Management Interface of the controller with an IP address of 172.16.1.40 and the Management Interface of the controller with an IP address of

172.16.1.30.



Once the CPU ACL is created, you need to apply it to the WLC. Enter these commands from the WLC CLI in order to apply the CPU ACL to the WLC:

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

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

Enter this command in order to disable the CPU ACL:

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

Note: This example gives an illustration of how to configure the rules to permit LWAPP and mobility traffic only. When you create the rules for the ACL, ensure that all protocols that are required on the WLAN are permitted because there is an implicit deny at the end of every ACL.

Verify

Cisco recommends that you test your ACL configurations with a wireless client in order to ensure that you have configured them correctly. If they fail to operate correctly, verify the ACLs on the ACL web page and verify that your ACL changes were applied to the controller's interface.

You can also use these **show** commands in order to verify your configuration:

- **show acl summary** In order to display the ACLs that are configured on the controller, use the **show acl summary** command.

  Here is an example:

```
(Cisco Controller) >show acl summary

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

- **show acl detailed** *ACL_Name* Displays detailed information on the configured ACLs.

  Here is an example:

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

                    Source                        Destination                Source P
I  Dir       IP Address/Netmask             IP Address/Netmask        Prot    Range
-- --- ------------------------------ ------------------------------ ---- --------
 1  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17    68-68
 2 Out      172.16.1.1/255.255.255.255       0.0.0.0/0.0.0.0           17    67-67
 3 Any         0.0.0.0/0.0.0.0               0.0.0.0/0.0.0.0            1     0-65
 4  In         0.0.0.0/0.0.0.0             172.16.1.1/255.255.255.255   17     0-65
 5 Out      172.16.1.1/255.255.255.255       0.0.0.0/0.0.0.0           17    53-53
 6  In         0.0.0.0/0.0.0.0             172.18.0.0/255.255.0.0             60-65
 7 Out      172.18.0.0/255.255.0.0           0.0.0.0/0.0.0.0            6    23-23
```

- **show acl cpu** In order to display the ACLs configured on the CPU, use the **show acl cpu** command.

  Here is an example:

```
(Cisco Controller) >show acl cpu

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

Troubleshoot

Controller software release 4.2.61.0 or later enables you to configure ACL counters. ACL counters can assist in determining which ACLs were applied to packets transmitted through the controller. This feature is useful when you troubleshoot your system.

ACL counters are available on these controllers:

- 4400 Series
- Cisco WiSM
- Catalyst 3750G Integrated Wireless LAN Controller Switch

In order to enable this feature, complete these steps:

1. Click **Security** > **Access Control Lists** > **Access Control Lists** in order to open the Access Control Lists page.

   This page lists all of the ACLs that have been configured for this controller.
2. In order to see if packets are hitting any of the ACLs configured on your controller, check the **Enable Counters** check box and click **Apply**. Otherwise, leave the check box unchecked. This is the default value.

3. If you want to clear the counters for an ACL, hover your cursor over the blue drop−down arrow for that ACL and choose **Clear Counters**.

Related Information

- **Configuring and Applying Access Control Lists**
- **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**

Updated: Jan 21, 2008 Document ID: 71978