This section describes how to configure access control lists (ACLs) for the Cisco 4700 Series Application Control Engine (ACE) appliance.

Contents

Overview

After reading this section, you should have a basic understanding of how to configure an access control list in an ACE to secure your network.

You can use ACLs with the ACE appliance to permit or deny traffic to or from a specific IP address or an entire network. For example, you can permit all e mail traffic on a circuit, but block Telnet traffic. You can also use ACLs to allow one client to access a part of the network while preventing other clients from doing so.

You must configure an ACL on each interface that you want to permit connections. Otherwise, the ACE will deny all traffic on the interface. An ACL consists of a series of ACL entries, which are permit-or-deny entries with criteria for the source IP address, destination IP address, protocol, port, or protocol-specific

parameters. Each entry permits or denies inbound or outbound network traffic to the parts of your network specified in the entry.

The order of the ACL entries is important. When the ACE decides whether to accept or refuse a connection, it tests the packet against each ACL entry in the order in which the entries are listed. After it finds a match, it stops checking entries.

For example, if you create an entry at the beginning of an ACL that explicitly permits all traffic, the ACE skips any other entries in the ACL. An implicit deny all entry exists at the end of every ACL, so you must include entries for every interface on which you want to permit connections. Otherwise, the ACE appliance will deny all traffic on the interface.

Certain applications require special handling of the data portion of a packet as the packets pass through the ACE. The ACE verifies the protocol behavior and identifies unwanted or malicious traffic that attempts to pass through. Based on the specifications of the traffic policy, the ACE performs application protocol inspection to accept or reject the packet to ensure the secure use of applications and services.

For more information on how to configure an ACL to permit or deny specific traffic or resources, see the Cisco ACE 4700 Series Appliance Security Configuration Guide.

The basic steps in configuring an ACL include:

- Creating an ACL
- Adding at least one ACL entry to the ACL
- Associating the ACL with an interface

To configure an ACL, you can use either the ACE Device Manager user interface (GUI) or the CLI.

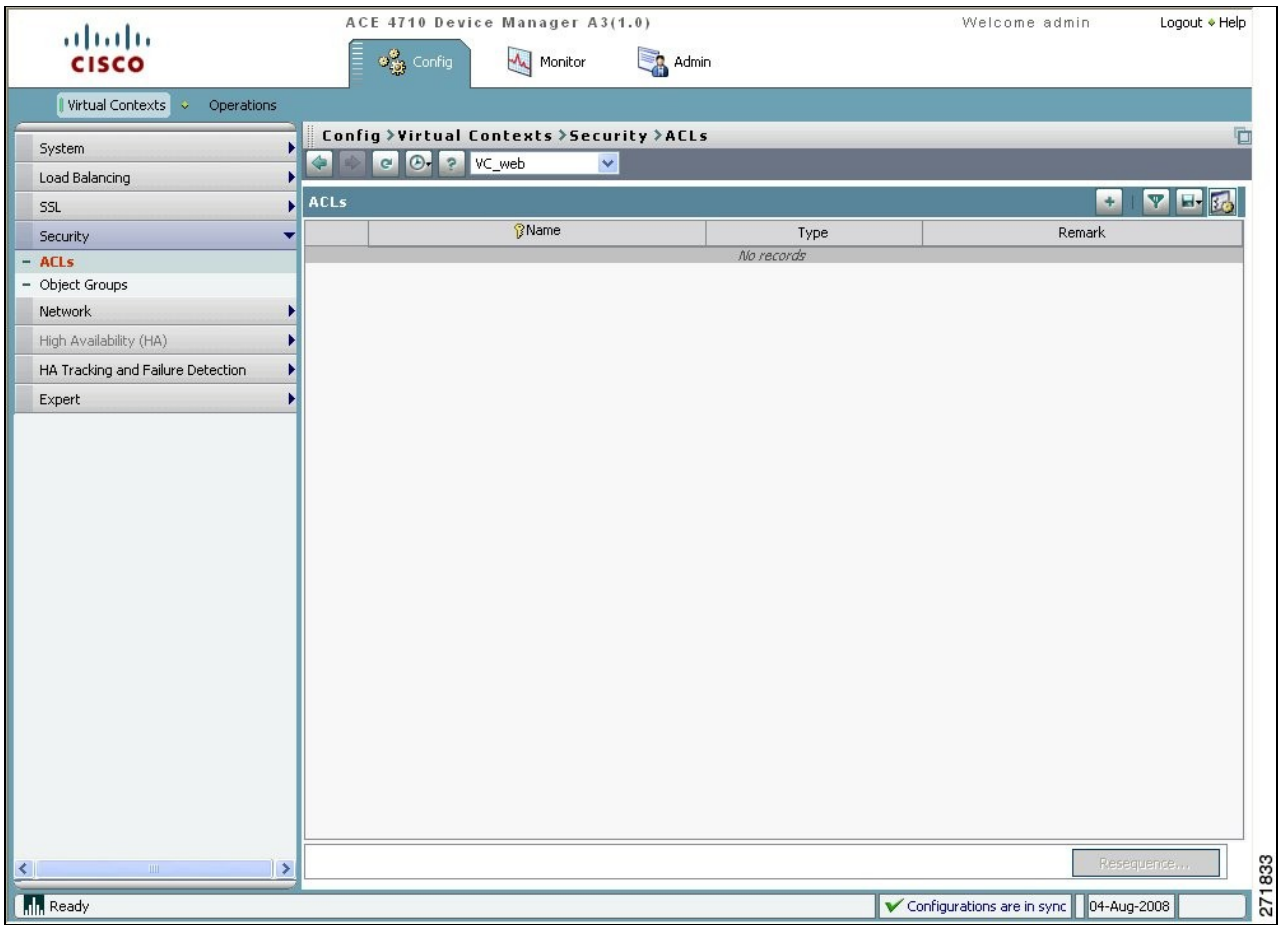
Configuring an ACL Using the Device Manager GUI

Configure an ACL using the ACE Device Manager GUI by following these steps:

1. Choose **VC_web**.

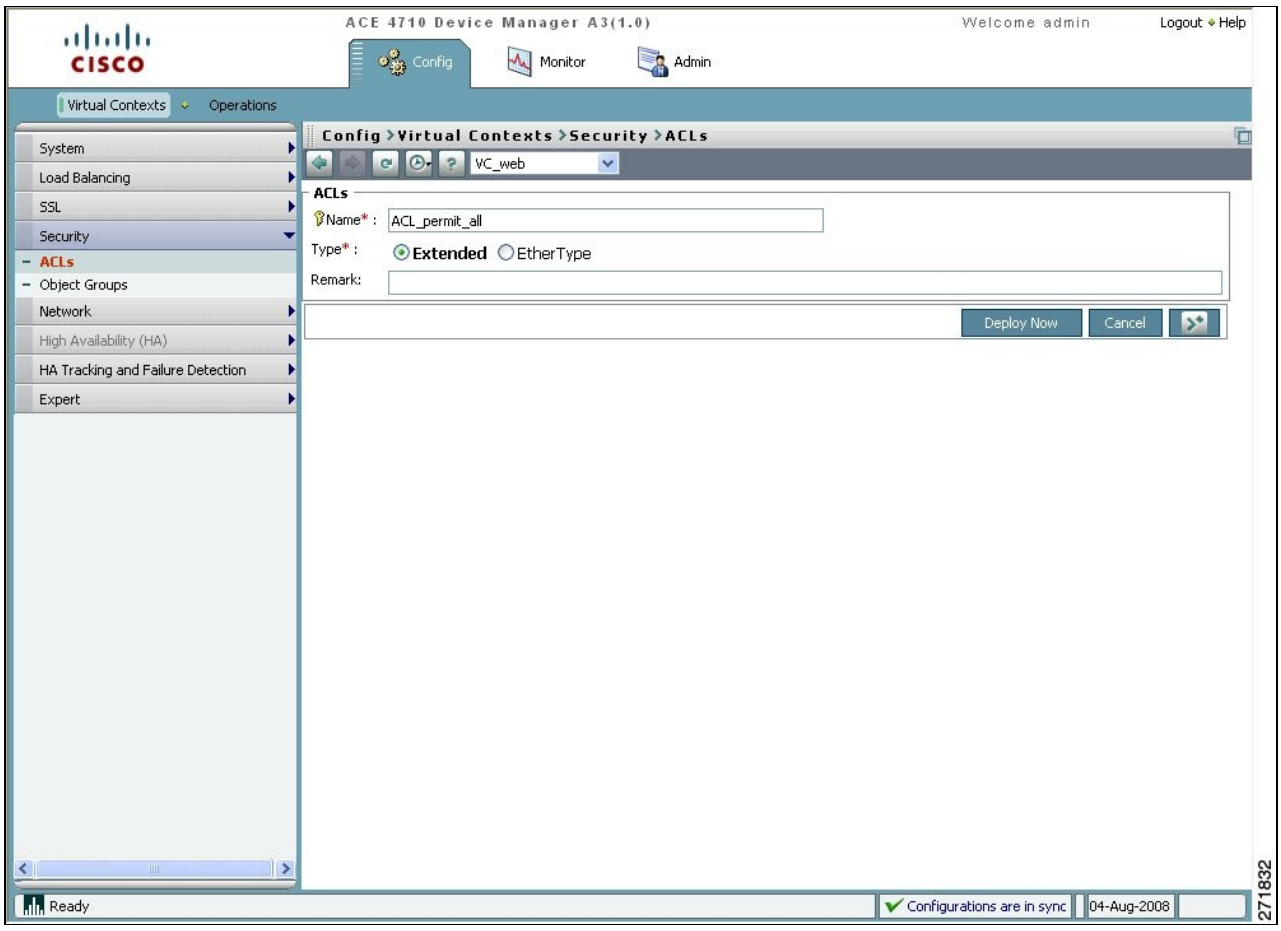
2. Choose **Config > Virtual Contexts > Security > ACLs**. The ACLs pane appears, listing the existing ACLs (Figure 1).

Figure 1 ACLs Pane



3. Click **Add** to create an ACL. The ACL configuration window appears (Figure 2).

Figure 2 ACL Configuration Window



4. Enter the following ACL properties. Leave the remaining properties blank or with the default values.

   ◊ Name: ACL_permit_all

   ◊ Type: Extended

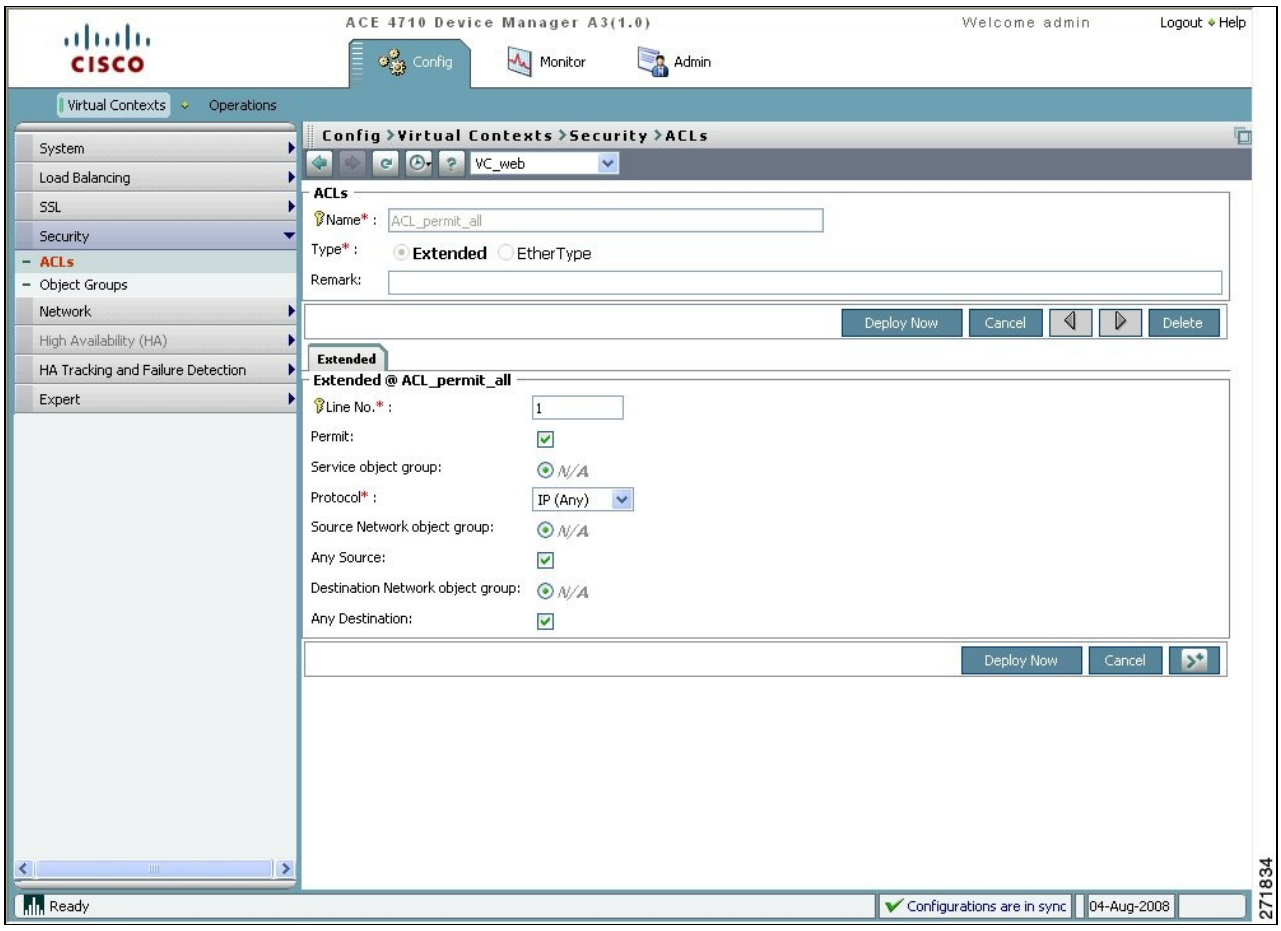
   ? Extended?Control network access for IP traffic

   ? EtherType?Control network access for non-IP traffic

5. Click **Deploy Now**. The Extended pane appears.

6. Click **Add** to create an ACL entry. The ACL entry configuration window appears (Figure 3).

Figure 3 ACL Entry Configuration Window



7. Create an ACL entry with the following attributes. Leave the remaining attributes blank or with the default values.

◊ Line No.: 1

Note For easier insertion of additional ACL entries later, you can enter non-sequential line numbers such as 10, 20, and so on.

◊ Permit: (Checked)

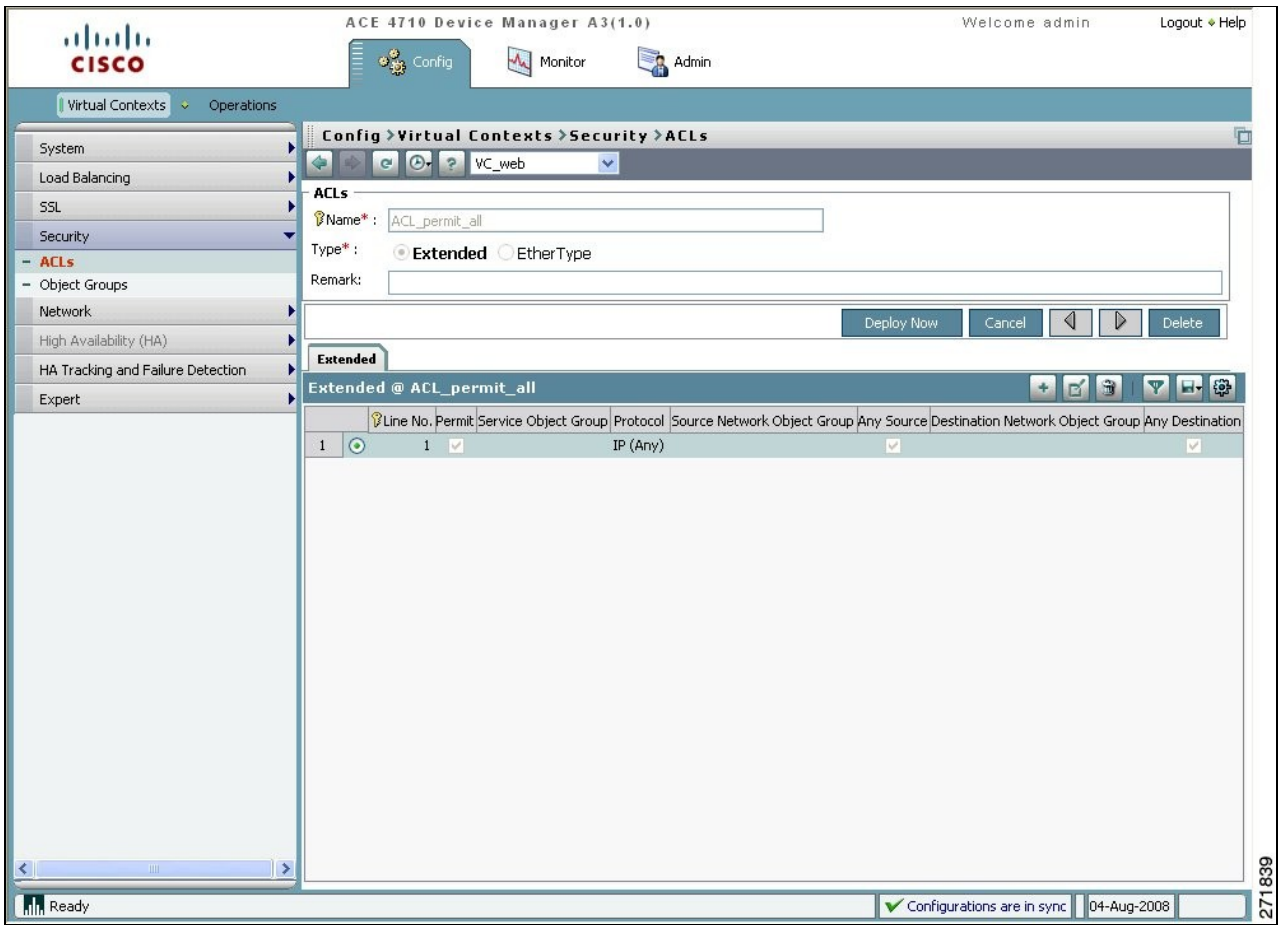
◊ Protocol: IP (Any)

◊ Any Source: (Checked)

◊ Any Destination: (Checked)

8. Click **Deploy Now** to save the ACL entry on the virtual context. The ACL entry is added to the Extended @ ACL_permit_all pane (Figure 4).

Figure 4 ACL Entry is Added

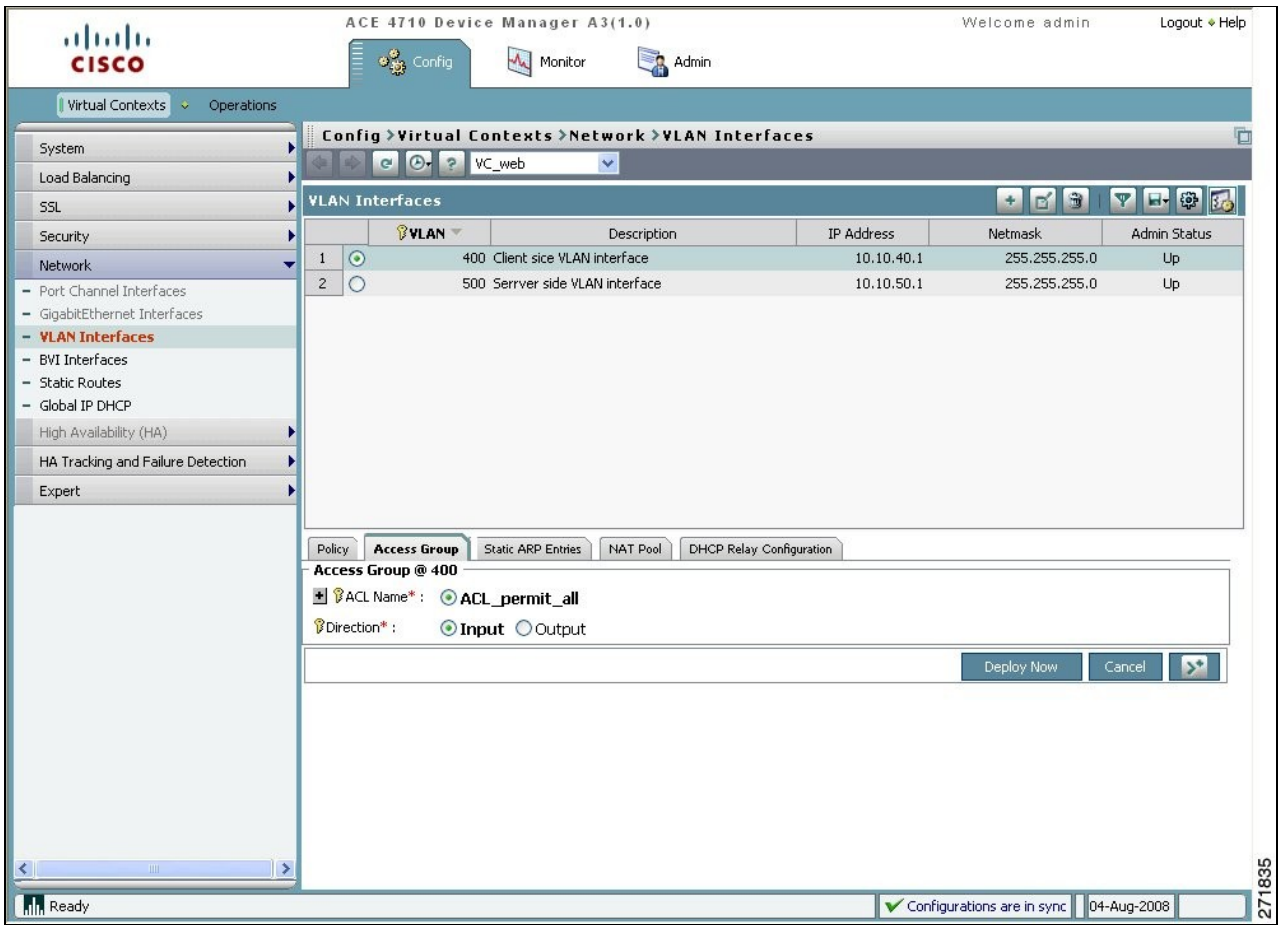


9. Choose **Network > VLAN Interfaces**. The VLAN Interfaces pane appears.

10. Choose the **Access Group** tab.

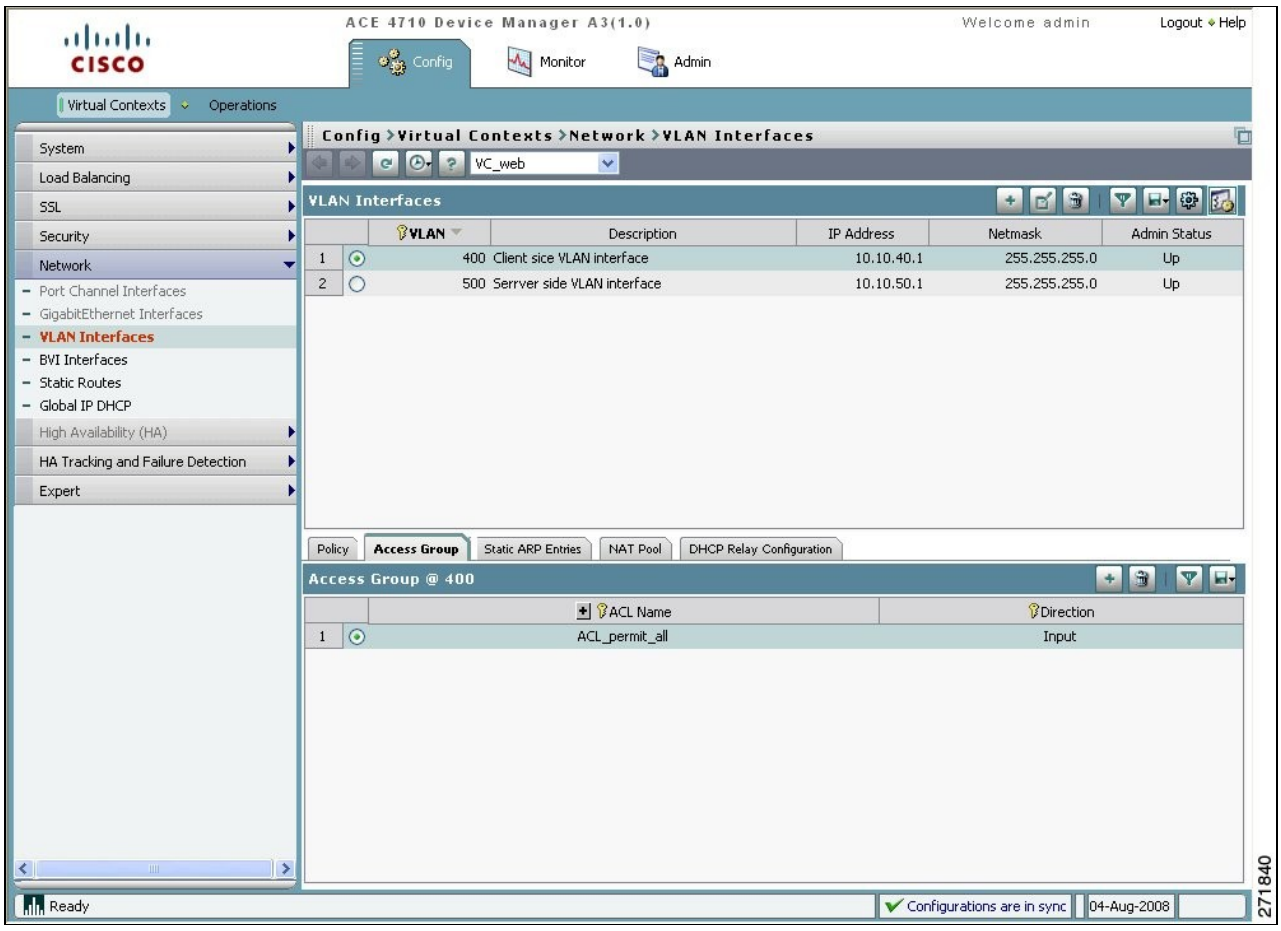
11. Click **Add** above the pane (Figure 5).

Figure 5 Adding an ACL to an Interface



Step 12 Click **Deploy Now** to accept the defaults and add an ACL to the interface. The ACL is added in the Access Group pane (Figure 6).

Figure 6 ACL is Added to an Interface



Configuring an ACL Using the CLI

You can configure an ACL using the command-line interface (CLI) by following these steps:

1. Check the CLI prompt to verify that you are operating in the desired context; change to the correct context if necessary.

```
host1/Admin# changeto VC_web

host1/VC_web#
```

2. Enter configuration mode.

```
host1/VC_web# Config

host1/VC_web(config)#
```

3. Create an ACL.

```
host1/VC_web(config)# access-list INBOUND extended permit ip any any
```

4. Apply the ACL to an interface.

```
host1/VC_web(config)# ???interface vlan 400???

host1/VC_web(config-if)# access-group input INBOUND

host1/VC_web(config-if)# exit
```

5. Display the ACL configuration information.

```
host1/VC_web(config)# exit

host1/VC_web# show running-config access-list
```

In this section, you have created an ACL entry to permit all traffic to the network. Next, you will create a user who is allowed to perform a subset of the ACE management functions on part of your network resources.