



#### Cisco 4700 Series Application Control Engine Appliance Quick Start Guide

Software Version A3(1.0)

#### **Americas Headquarters**

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883

Text Part Number: OL-17506-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Cisco 4700 Series Application Control Engine Appliance Quick Start Guide Copyright © 2008, Cisco Systems, Inc. All rights reserved.



#### CONTENTS

#### Preface vii

Audience viii How to Use This Guide viii Related Documentation ix Symbols and Conventions xii Obtaining Documentation and Submitting a Service Request 2-xiv Notices 2-xv OpenSSL/Open SSL Project 2-xv License Issues 2-xv xviii

#### CHAPTER 1

#### Overview 1-1

ACE Technologies 1-2 Setting Up an ACE Appliance 1-3 Creating Virtual Contexts 1-3 Configuring Access Control Lists 1-4 Configuring Role-Based Access Control 1-4 Configuring a Virtual Server 1-4 Configuring a Load-Balancing Predictor 1-6 Configuring Server Persistence Using Stickiness 1-6 Configuring SSL Security 1-7 Configuring Health Monitoring Using Health Probes 1-7

CHAPTER 2	Setting Up an ACE Appliance 2-1
	Overview 2-1
	Establishing a Console Connection on the ACE 2-4
	Enabling Management Connectivity Using the Setup Script 2-8
	Assigning a Name to the ACE 2-12
	Setting Up an ACE Appliance Using the Device Manager GUI 2-12 Logging in to the ACE 2-12
	Configuring a Second Gigabit Ethernet Interface Port <b>2-15</b> Configuring a Third Gigabit Ethernet Interface Port <b>2-19</b>
	Setting Up an ACE Appliance Using the CLI 2-21 Logging in to the ACE 2-21
	Configuring the First Gigabit Ethernet Port 2-22
	Allocating the First Gigabit Ethernet Port to a VLAN 2-23
	Configuring a Management VLAN Interface on the ACE 2-24
	Configuring a Second Gigabit Ethernet Interface Port 2-26
	Configuring a Third Gigabit Ethernet Interface Port 2-27
	Configuring Remote Management Access to the ACE 2-27
	Accessing the ACE through a Telnet Session 2-30
CHAPTER <b>3</b>	Creating a Virtual Context 3-1
	Overview 3-1
	Creating a Virtual Context Using the Device Manager GUI 3-3 Creating a Resource Class 3-4 Creating a Virtual Context 3-7
	Configuring the Client-Side VLAN Interface 3-12
	Configuring the Server-Side VLAN Interface 3-12
	Creating a Virtual Context Using the CLI 3-21
	Configuring a Resource Class 3-21
	Creating a Virtual Context 3-22

Cisco 4700 Series Application Control Engine Appliance Quick Start Guide

	Configuring a Management VLAN Interface to the User Context <b>3-23</b> Configuring Remote Management Access to the User Contexts <b>3-24</b> Configuring the Client-Side VLAN Interface <b>3-26</b> Configuring the Server-Side VLAN Interface <b>3-27</b>
CHAPTER <b>4</b>	Configuring Access Control Lists 4-1
	Overview 4-1
	Configuring an ACL Using the Device Manager GUI 4-2
	Configuring an ACL Using the CLI 4-9
CHAPTER 5	Configuring Role-Based Access Control 5-1
	Overview 5-1
	Configuring RBAC Using the Device Manager GUI 5-5
	Configuring RBAC Using the CLI 5-10
CHAPTER <b>6</b>	Configuring Server Load Balancing 6-1
	Overview 6-1
	Configuring Layer 7 Server Load Balancing Using the Device Manager GUI 6-3
	Configuring Layer 7 Server Load Balancing Using the CLI 6-10
	Configuring Real Servers 6-10
	Creating a Server Farm 6-11
	Creating a Virtual Server Traffic Policy 6-13
CHAPTER <b>7</b>	Configuring a Load-Balancing Predictor 7-1
	Overview 7-1
	Configuring a Hash Header Predictor Using the Device Manager GUI 7-3
	Configuring a Hash Header Predictor Using the CLI 7-4

L

CHAPTER 8	Configuring Server Persistence Using Stickiness 8-1
	Overview 8-1
	Configuring HTTP Cookie Stickiness Using the Device Manager GUI 8-4
	Configuring HTTP Cookie Stickiness Using the CLI 8-7
CHAPTER <b>9</b>	Configuring SSL Security 9-1
	Overview 9-1
	Configuring SSL Termination 9-4
	Configuring the ACE for SSL Termination Using the Device Manager GUI 9-6
	Configuring the ACE for SSL Termination Using the CLI 9-14
CHAPTER 10	Configuring Health Monitoring Using Health Probes 10-1
	Overview 10-1
	Configuring an HTTP Health Probe Using the Device Manager GUI 10-3
	Configuring an HTTP Health Probe Using the CLI <b>10-7</b>
INDEX	—



# Preface

This guide provides the following information:

- An overview of the major functions and features of the Cisco 4700 Series Application Control Engine (ACE) appliance
- Instructions on how to initially configure the ACE to allow traffic and basic load balancing
- Instructions on how to configure the ACE to provide various scalability and security capabilities
- References to find the information in the documentation set

This preface contains the following major sections:

- Audience
- How to Use This Guide
- Related Documentation
- Symbols and Conventions
- Obtaining Documentation and Submitting a Service Request
- Open Source License Acknowledgements

### Audience

This guide is intended for the following trained and qualified service personnel who are responsible for configuring the ACE:

- Web master
- System administrator
- System operator

### How to Use This Guide

This guide is organized as follows:

Chapter	Description	
Chapter 1, Overview	Provides an overview of the major functions and features of the ACE	
Chapter 2, Setting Up an ACE Appliance	Provides procedures to initially configure the ACE to allow the passing of traffic and remote access	
Chapter 3, Creating a Virtual Context	Provides procedures to partition the ACE into virtual contexts for more efficient operation	
Chapter 4, Configuring Access Control Lists	Provides procedures to configure an access control list in an ACE to secure your network	
Chapter 5, Configuring Role-Based Access Control	Provides procedures to configure a user with permission to perform limited operations and access a subset of your network	
Chapter 6, Configuring Server Load Balancing	Provides procedures to configure the ACE to allow basic server load balancing	
Chapter 7, Configuring a Load-Balancing Predictor	Provides procedures to select a predefined predictor for server load balancing	
Chapter 8, Configuring Server Persistence Using Stickiness	Provides procedures to configure server persistence for requests from a client using stickiness	

Chapter	Description
Chapter 9, Configuring SSL Security	Provides procedures to configure SSL security for your network
Chapter 10, Configuring Health Monitoring Using Health Probes	Provides procedures to configure server health monitoring using health probes

If you are already familiar with the ACE appliance and would like to quickly set up the device for basic server load balancing, you can follow the configuration procedures in the following chapters:

- Chapter 2, Setting Up an ACE Appliance
- Chapter 3, Creating a Virtual Context
- Chapter 6, Configuring Server Load Balancing

The remaining chapters allow you to explore additional capabilities of the ACE.

### **Related Documentation**

In addition to this document, the ACE documentation set includes the following documents:

Document Title	Description	
Release Note for the Cisco 4700 Series Application Control Engine Appliance	Provides information about operating considerations, caveats, and CLI commands for the ACE appliance.	
Cisco 4710 Application Control Engine Appliance Hardware Installation Guide	Provides information for installing the ACE appliance.	

Document Title	Description
Cisco 4700 Series Application Control Engine Appliance Device Manager GUI Configuration Guide	Describes how to configure the ACE using the Device Manager GUI and provides background details about the attributes used in the GUI.
Cisco 4700 Series Application Control Engine Appliance Command Reference	Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.
Cisco 4700 Series Application Control Engine Appliance Administration Guide	<ul> <li>Describes how to perform the following administration tasks on the ACE:</li> <li>Setting up the ACE</li> <li>Establishing remote access</li> <li>Managing software licenses</li> <li>Configuring class maps and policy maps</li> <li>Managing the ACE software</li> <li>Configuring SNMP</li> <li>Configuring redundancy</li> <li>Configuring the XML interface</li> <li>Upgrading the ACE software</li> </ul>
Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide	Describes how to operate your ACE in a single context or in multiple contexts and how to configure Role-Based Access Control.

Document Title	Description		
Cisco 4700 Series Application Control	Describes how to configure the following routing and bridging tasks on the ACE:		
Engine Appliance Routing and Bridging	• VLAN interfaces		
Configuration Guide	• Routing		
	• Bridging		
	Dynamic Host Configuration Protocol (DHCP)		
Cisco 4700 Series Application Control	Describes how to configure the following server load-balancing tasks on the ACE:		
Engine Appliance Server	• Real servers and server farms		
Load-Balancing Configuration Guide	• Class maps and policy maps to load-balance traffic to real servers in server farms		
	• Server health monitoring (probes)		
	• Stickiness		
	Firewall load balancing		
	TCL scripts		
Cisco 4700 Series Application Control	Describes how to perform the following ACE security configuration tasks:		
Engine Appliance Security	Access control lists (ACLs)		
Configuration Guide	• User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server		
	• Application protocol and HTTP deep packet inspection		
	• TCP/IP normalization and termination parameters		
	• Network address translation (NAT)		

Document Title	Description	
Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide	Describes how to configure the following SSL tasks on the ACE: • SSL certificates and keys • SSL initiation • SSL termination • End-to-end SSL	
Cisco 4700 Series Application Control Engine Appliance System Message Guide	Describes how to configure system message logging on the ACE. This guide also lists and describes the system log (syslog) messages generated by the ACE.	
Cisco CSM-to-ACE Conversion Tool User Guide	Describes how to use the CSM-to-ACE conversion tool to migrate Cisco Content Switching Module (CSM) running or startup configuration files to the ACE.	
Cisco CSS-to-ACE Conversion Tool User Guide	Describes how to use the CSS-to-ACE conversion tool to migrate Cisco Content Services Switches (CSS) running or startup configuration files to the ACE.	

# **Symbols and Conventions**

This publication uses the following conventions:

Convention	Description	
<b>boldface</b> font	Commands, command options, and keywords are in <b>boldface</b> . Bold text also indicates a command in a paragraph.	
italic font	Arguments for which you supply values are in <i>italics</i> .	
[]	Elements in square brackets are optional.	
$\{ x \mid y \mid z \}$	Alternative keywords are grouped in braces and separated by vertical bars.	

Convention	Description	
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.	
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.	
screen font	Terminal sessions and information the system displays are in screen font.	
<b>boldface screen</b> font	Information you must enter on a command line is in <b>boldface screen</b> font.	
italic screen font	Arguments for which you supply values are in <i>italic screen</i> font.	
۸	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.	
< >	Nonprinting characters, such as passwords are in angle brackets.	

- 1. A numbered list indicates that the order of the list items is important.
  - **a**. An alphabetical list indicates that the order of the secondary list items is important.
- A bulleted list indicates that the order of the list topics is unimportant.
  - An indented list indicates that the order of the list subtopics is unimportant.

Notes use the following conventions:



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:



Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

### **Notices**

The following notices pertain to this software license.

#### **OpenSSL/Open SSL Project**

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

#### License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

#### **OpenSSL License:**

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

- 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
- Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
- 6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

#### **Original SSLeay License:**

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the

SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- **3**. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,

#### OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Cisco 4700 Series Application Control Engine Appliance Quick Start Guide



# CHAPTER

## **Overview**

The Cisco 4700 Series Application Control Engine (ACE) appliance performs server load balancing, network traffic control, service redundancy, resource management, encryption and security, and application acceleration and optimization, all in a single network appliance.

This chapter contains a high-level introduction to the following topics:

- ACE Technologies
- Setting Up an ACE Appliance
- Creating Virtual Contexts
- Configuring Access Control Lists
- Configuring Role-Based Access Control
- Configuring a Virtual Server
- Configuring a Load-Balancing Predictor
- Configuring Server Persistence Using Stickiness
- Configuring SSL Security
- Configuring Health Monitoring Using Health Probes

# **ACE Technologies**

Server load balancing helps ensure the availability, scalability, and security of applications and services by distributing the work of a single server across multiple servers.

When you configure server load balancing on your ACE appliance, the ACE decides which server should receive a client request such as a web page or a file. The ACE selects a server that can successfully fulfill the client request most effectively, without overloading the selected server or the overall network.

Table 1-1 shows the ACE technologies that provide network availability, scalability, and security at both the device and network services levels.

Level	Availability	Scalability	Security	
Device	Device Setup	Virtual Contexts	Access Control Lists	
		Role-Based Ac	Role-Based Access Control	
Network Services	Virtual Servers	Load Balancing Predictors	SSL	
	Health Probes	Server Persistence Using Stickiness	Access Control Lists	
	Role-Based Acc		cess Control	

#### Table 1-1 ACE Technologies

At the device level, the ACE provides high network availability by supporting:

- Device redundancy—The high availability support of the ACE allows you to set up a peer ACE device to the configuration so that if one ACE becomes inoperative, the other ACE can take its place immediately.
- Scalability—Supports virtualization by partitioning one ACE device into independent virtual devices, each with its own resource allocation.
- Security—Supports access control lists which restrict access from certain clients or to certain network resources.

At the network service level, the ACE provides:

- High services availability—Supports high-performance server load balancing, which distributes client requests among physical servers and server farms, and provides health monitoring at the server and server farm levels through implicit and explicit health probes.
- Scalability—Supports virtualization using advanced load-balancing algorithms (predictors) to distribute client requests among the virtual devices configured in the ACE. Each virtual device includes multiple virtual servers. Each server forwards client requests to one of the server farms. Each server farm can contain multiple physical servers.

Although the ACE can distribute client requests among hundreds or even thousands of physical servers, it can also maintain server persistence. With some e-commerce applications, all client requests within a session are directed to the same physical server so that all the items in one shopping cart are contained on one server.

• Services-level security—Establishes and maintains a Secure Sockets Layer (SSL) session between the ACE and its peer which provides secure data transactions between clients and servers.

# Setting Up an ACE Appliance

To set up an ACE appliance, you first establish a connection to the ACE and perform the initial device setup required to prepare the ACE for providing application networking services. For more information, see Chapter 2, "Setting Up an ACE Appliance."

### **Creating Virtual Contexts**

Next, you partition the ACE device into multiple virtual contexts, each with its own resource allocation. For more information, see Chapter 3, "Creating a Virtual Context."

## **Configuring Access Control Lists**

Then, you control access to your network resources to guarantee that only desired traffic passes through, and that the appropriate users can access the network resources they need.

You use Access Control Lists (ACLs) to secure your network by permitting or denying traffic to or from a specific IP address or an entire network.

You must configure an ACL for each interface on which you want to permit connections. Otherwise, the ACE will deny all traffic on that interface. An ACL consists of a series of ACL 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.

This guide provides an example of ACL configuration at the device level (see Chapter 4, "Configuring Access Control Lists"). To learn how to configure ACL at the network services level, or how to configure more granular access control security, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

### **Configuring Role-Based Access Control**

You can manage the complexity of large-network security administration by defining the commands and resources available to each user through Role-Based Access Control (RBAC). RBAC supports network security at both the device and network services levels by defining physical or virtual resources in a domain that the user can access.

For more information, see Chapter 5, "Configuring Role-Based Access Control."

### **Configuring a Virtual Server**

You can configure a virtual server to intercept web traffic to a website and allow multiple real servers (physical servers) to appear as a single server for load-balancing purposes.

\_

Table 1-2 illustrates how the ACE supports scalability through virtual contexts, virtual servers, server farms, and real servers.

Table 1-2ACE Scalability

				Real Server A1
	Virtual Context 1	Virtual Server A	Server Farm A	Real Server A2
			Backup Server Farm a	Real Server An
				Real Server a1
				Real Server a2
		Virtual Server B	Server Farm B	Real Server an
				Real Server B1
ACE				Real Server B2
	Virtual Context 2	Virtual Server C	Server Farm C	Real Server Bn
				Real Server C1
				Real Server C2
		Virtual Server D	Server Farm D	Real Server Cn
				Real Server D1
				Real Server D2
				Real Server Dn

You can partition your ACE into multiple virtual contexts, each of which has its own set of policies, interfaces, and resources. A virtual server is bound to physical resources that run on a real server in a server farm.

Real servers relate to the actual, physical servers on your network. They can be configured to provide client services or as backup servers.

Related real servers are grouped into server farms. Servers in the same server farm often contain identical content (referred to as mirrored content) so that if one server becomes inoperative, another server can take over its functions immediately. Mirrored content also allows several servers to share the load during times of increased demand.

For more information, see Chapter 6, "Configuring Server Load Balancing."

### **Configuring a Load-Balancing Predictor**

To distribute incoming client requests among the servers in a server farm, you define load-balancing rules called predictors using IP address and port information.

When there is a client request for an application service, the ACE performs server load balancing by deciding which server can successfully fulfill the client request in the shortest amount of time without overloading the server or server farm. Some sophisticated predictors take into account factors such as a server's load, response time, or availability, allowing you to adjust load balancing to each application's particular past.

For more information, see Chapter 7, "Configuring a Load-Balancing Predictor."

### **Configuring Server Persistence Using Stickiness**

You can configure the ACE to allow the same client to maintain multiple simultaneous or subsequent TCP or IP connections with the same real server for the duration of a session. A session is defined as a series of interactions between a client and a server over some finite period of time (from several minutes to several hours). Cisco calls this server persistence feature stickiness.

Many network applications require that customer-specific information be stored persistently across multiple server requests. A common example is a shopping cart used on an e-commerce site. With server load balancing in use, it could potentially be a problem if a back-end server needs information generated at a different server during a previous request.

Depending on how you have configured server load balancing, the ACE sticks a client to an appropriate server after it has determined which load-balancing method to use. If the ACE determines that a client is already stuck to a particular

server, then the ACE sends subsequent client requests to that server, regardless of the load-balancing criteria. If the ACE determines that the client is not stuck to a particular server, it applies the normal load-balancing rules to the request.

The combination of the predictor and stickiness enables the application to have scalability, availability, and performance even with persistence for transaction processing.

For more information, see Chapter 8, "Configuring Server Persistence Using Stickiness."

### **Configuring SSL Security**

Use the SSL security protocol for authentication, encryption, and data integrity in a Public Key Infrastructure (PKI).

SSL configuration in an ACE establishes and maintains an SSL session between the ACE and its peer, enabling the ACE to perform its load-balancing tasks on the SSL traffic. These SSL functions include server authentication, private-key and public-key generation, certificate management, and data packet encryption and decryption.

For more information, see Chapter 9, "Configuring SSL Security."

## **Configuring Health Monitoring Using Health Probes**

Application services require monitoring to ensure availability and performance. You can configure the ACE to track the health and performance of your servers and server farms by creating health probes. Each health probe that you create can be associated with multiple real servers or server farms.

When you enable ACE health monitoring, the appliance periodically sends messages to the server to determine server status. The ACE verifies the server's response to ensure that a client can access that server. The ACE can use the server's response to place the server in or out of service. In addition, the ACE can use the health of servers in a server farm to make reliable load-balancing decisions.

For more information, see Chapter 10, "Configuring Health Monitoring Using Health Probes."

Configuring Health Monitoring Using Health Probes



# **CHAPTER 2**

# Setting Up an ACE Appliance

This chapter describes how to set up a Cisco 4700 Series Application Control Engine (ACE) appliance. It includes the following major sections:

- Overview
- Establishing a Console Connection on the ACE
- Enabling Management Connectivity Using the Setup Script
- Assigning a Name to the ACE
- Setting Up an ACE Appliance Using the Device Manager GUI
- Setting Up an ACE Appliance Using the CLI

### **Overview**

After reading this chapter, you should have a basic understanding of how to configure a ACE appliance with the networking parameters necessary for communicating with a management device to configure server load balancing.

After some initial setup using the CLI, you can complete the procedures in this chapter using the Device Manager GUI.

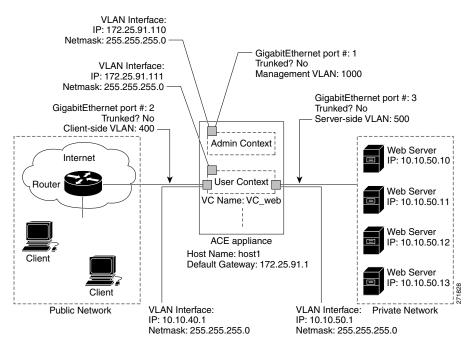
Before performing the procedures in this section, make sure that you complete the ACE installation instructions as described in the *Cisco 4710 Application Control Engine Appliance Hardware Installation Guide*.

Configuring an ACE involves the following basic steps:

- **Step 1** Establishing a console connection on the ACE.
- Step 2 Enable management connectivity to the ACE through a Gigabit Ethernet port.
- Step 3 Log in to the ACE.
- Step 4 Configure a second Gigabit Ethernet port for client-side connectivity.
- Step 5 Configure a third Gigabit Ethernet port for server-side connectivity.

This chapter describes how to set up an ACE appliance using the example network setup illustrated in Figure 2-1.





The configuration of the example setup is as follows:

• VLAN 1000 is assigned to the first Gigabit Ethernet port and is used for management traffic for both the Admin context and a user context.



- **Note** A virtual local area network (VLAN) is a logical division of a computer network within which information can be transmitted for all devices to receive. VLANs enable you to segment a switched network so that devices in one VLAN do not receive information packets from devices in another VLAN.
- VLAN 400 is assigned to the second Gigabit Ethernet port and is used for client-side traffic.
- VLAN 500 is assigned to the third Gigabit Ethernet port and is used for server-side traffic.
- None of the three Gigabit Ethernet ports used are trunked.
- A management VLAN interface is configured for the Admin context with VLAN 1000 and IP address 172.25.91.110.
- A management VLAN interface is configured for the user context VC\_web with VLAN 1000 and IP address 172.25.91.111.
- A client-side VLAN interface is configured for the user context VC\_web with VLAN 400 and IP address 10.10.40.10.
- A server-side VLAN interface is configured for the user context VC\_web with VLAN 500 and IP address 10.10.50.1.
- Four web servers are available to the ACE for load-balancing client requests.

# **Establishing a Console Connection on the ACE**

The ACE has one standard RS-232 serial port on its rear panel that operates as the console port. You can establish a direct serial connection between the ACE and your terminal (or a PC with terminal software) by making a serial connection to this console port. The integrated serial port accepts a 9-pin female D-shell connector. Use a straight-through cable to connect the ACE to the terminal or a PC. For more instructions on connecting a console cable to your ACE appliance, see the *Cisco 4710 Application Control Engine Appliance Hardware Installation Guide*.

The ACE appliance has four physical Ethernet interface ports. All VLANs are assigned to these ports. The four Ethernet ports provide the physical connection between the ACE and the servers, PCs, routers, and other devices. You can configure the Ethernet ports to provide an interface for connecting to 10-Mbps, 100-Mbps, or 1000-Mbps networks. After the VLANs are assigned, you can configure the corresponding VLAN interfaces so that the ACE can provide different networking functions for different VLANs.



Only the Admin context is directly accessible through the console port; all other contexts can be accessed through Telnet or SSH sessions on the Ethernet ports.

After making the console connection, you can use any terminal communications application to access the ACE CLI.



If the appliance is not on, press the power button on the front of the ACE to start the boot process. See the *Cisco 4710 Application Control Engine Appliance Hardware Installation Guide* for details.

Access the ACE CLI using HyperTerminal for Windows by following these steps:

Step 1 Launch HyperTerminal.

The Connection Description window appears (Figure 2-2).

Figure 2-2 HyperTerminal—Connection Description



- Step 2 Enter a name for your connection in the Name field.
- Step 3 Click OK. The Connect To window appears (Figure 2-3).

Connect To				
🧞 4710 Console				
Enter details for the phone number that you want to dial:				
Country/region: United States (1)				
Area code: 1				
Phone number:				
Connect using: COM4				
OK Cancel	071855			

Figure 2-3 HyperTerminal—Connect To

- Step 4 From the Connect using drop-down list, choose the COM port to which the device is connected.
- Step 5 Click OK. The Port Properties window appears (Figure 2-4).

COM4 Properties	? 🔀		
Port Settings			
Bits per second:	9600		
Data kitu			
Data bits:	8		
Parity:	None		
Stop bits:	1		
Flow control:	None		
	Restore Defaults		
	Thestole Deladits		
OK Cancel Apply			

Figure 2-4 HyperTerminal—Port Properties

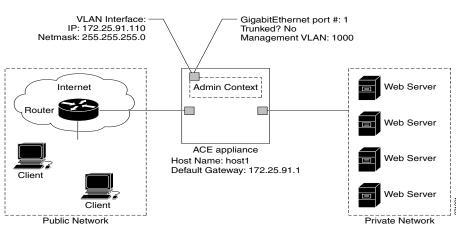
**Step 6** Set the port properties:

- Bits per second = 9600
- Data bits = 8
- Parity = none
- Stop bits = 1
- Flow control = None
- Step 7 Click OK to connect.

# Enabling Management Connectivity Using the Setup Script

When you boot the ACE for the first time and the ACE does not detect a startup configuration file, a setup script guides you through the process of configuring a management VLAN on the ACE through one of its Gigabit Ethernet ports to enable connectivity to the Device Manager GUI.

After running the setup script, the management VLAN is allocated to the specified Gigabit Ethernet port and the VLAN interface is configured on the ACE, as illustrated in Figure 2-5.



#### Figure 2-5 Configuration After the Setup Script is Executed

Configure the ACE using the setup script by following these steps:

Step 1 At the login prompt, log into the ACE by entering the login username admin and password. By default, the username and password are admin. For example, enter:

Starting sysmgr processes.. Please wait...Done!!!

switch login: **admin** Password: **admin**  Step 2 At the Enter the new password for "admin": prompt, change the default Admin password. If you do not change the default Admin password, after you upgrade the ACE software you will only be able to log in to the ACE through the console port.

Enter the new password for "admin": XXXXX Confirm the new password for "admin": XXXXX admin user password successfully changed.

Step 3 At the Enter the new password for "www": prompt, change the default www user password. If you do change the default www user password, the www user will be disabled and you will not be able to use Extensible Markup Language (XML) to remotely configure an ACE until you change the default www user password.

Enter the new password for "www": XXXXX Confirm the new password for "www": XXXXX www user password successfully changed.

This script will perform the configuration necessary for a user to manage the ACE Appliance using the ACE Device Manager. The management port is a designated Ethernet port which has access to the same network as your management tools including the ACE Device Manager. You will be prompted for the Port Number, IP Address, Netmask and Default Route (optional).

Enter 'ctrl-c' at any time to quit the script



**Caution** At this point, you should consider whether you plan to configure the ACE using the Device Manager GUI or using the CLI. If you have a trunking network setup, or if your VLAN 1000 has been used, you should bypass the following setup script and use the CLI at "Setting Up an ACE Appliance Using the CLI."

Step 4 At the "Would you like to enter the basic configuration dialog? (yes/no)" prompt, press Enter to continue the setup. To bypass setup and directly access the CLI, type no.

Would you like to enter the basic configuration dialog? (yes/no) [y]:

	<b>Note</b> The ACE provides a default response in brackets [] for each question in the setup script. Accept the default response to a configuration prompt by pressing <b>Enter</b> .			
Step 5	Select port 1 to carry management VLAN communication by pressing Enter.			
	Enter the Ethernet port number to be used as the management port (1-4):? [1]:			
Step 6	Assign an IP address for the management VLAN interface by entering <b>172.25.91.110</b> .			
	Enter the management port IP Address (n.n.n.n): [192.168.1.10]: 172.25.91.110			
Step 7	Accept the default subnet mask for the management VLAN interface by pressin <b>Enter</b> .			
	Enter the management port Netmask(n.n.n.n): [255.255.255.0]:			
Step 8	Assign the IP address of the gateway router (the next-hop address for this route by entering <b>172.25.91.1</b> .			
	Enter the default route next hop IP Address (n.n.n.n) or <enter> to skip this step: <b>172.25.91.1</b></enter>			
Step 9	Examine the entered values.			
	Summary of entered values:			
	Management Port: 1 Ip address 172.25.91.110 Netmask: 255.255.255.0 Default Route: 172.25.91.1			
Step 10	Review the configuration details by pressing <b>d</b> .			
	Submit the configuration including security settings to the ACE Appliance? (yes/no/details): [y]:			
	interface gigabitEthernet 1/3 switchport access vlan 1000 no shut			
	access-list ALL extended permit ip any any class-map type management match-any remote_access match protocol xml-https any			

#### Cisco 4700 Series Application Control Engine Appliance Quick Start Guide

```
match protocol dm-telnet any
 match protocol icmp any
 match protocol telnet any
 match protocol ssh any
 match protocol http any
 match protocol https any
 match protocol snmp any
policy-map type management first-match remote_mgmt_allow_policy
  class remote access
   permit
interface vlan 1000
  ip address 172.25.91.110 255.255.255.0
  access-group input ALL
 service-policy input remote_mgmt_allow_policy
 no shutdown
ssh kev rsa
ip route 0.0.0.0 0.0.0.0 172.25.91.1
```

#### Step 11 Accept this configuration by pressing Enter; otherwise, press n.

```
Submit the configuration including security settings to the ACE Appliance? (yes/no/details): [y]:
```

#### **Step 12** After you select **y**, the following message appears.

Configuration successfully applied. You can now manage this ACE Appliance by entering the url 'https://172.25.91.110' into a web browser to access the Device Manager GUI.

After you have completed the setup script, the command prompt appears.

switch/Admin#

After you specify a Gigabit Ethernet port, port mode, and management VLAN, the setup script automatically applies the following default configuration:

- A Management VLAN is allocated to the specified Ethernet port.
- An extended IP access list that allows IP traffic originating from any other host addresses.
- A traffic classification is created for management protocols HTTP, HTTPS, ICMP, SSH, Telnet, and XML-HTTPS. HTTPS is dedicated to connectivity with the Device Manager GUI.
- A VLAN interface is configured on the ACE.

# Assigning a Name to the ACE

The hostname is used for the command-line prompts and default configuration filenames. When you establish sessions to multiple devices, the hostname helps you keep track of which ACE you are entering commands to. By default, the hostname for the ACE is switch.

For example, change the hostname of the ACE from switch to host1 by entering:

```
switch/Admin# Config
switch/Admin(config)# hostname host1
```

The prompt appears with the new hostname.

```
host1/Admin(config)#
```

# Setting Up an ACE Appliance Using the Device Manager GUI

You can set up an ACE appliance using the Device Manager GUI or the CLI. This section describes how to set up an ACE using the GUI, and includes the following topics:

- Logging in to the ACE
- Configuring a Second Gigabit Ethernet Interface Port
- Configuring a Third Gigabit Ethernet Interface Port

# Logging in to the ACE

You can access the ACE Device Manager GUI through a web-based interface. Log in to the Device Manager by following these steps:

Step 1 Navigate to the ACE Device Manager by entering the secure HTTPS address or hostname of the ACE in the address field of a web browser. For the example setup shown earlier in Figure 2-1, enter:

```
https://172.25.91.110/
```

Step 2 Click Yes at the prompt to accept (trust) and install the signed certificate from Cisco Systems, Inc. To avoid having to approve the signed certificate every time you log in to the Device Manager, accept the certificate.

The Device Manager GUI Login window appears (Figure 2-6).

Note

Because this product is regularly updated, you may notice minor variations between the figures in this manual and the windows that appear in the software version you are running.

iliulu cisco	
ACE 4710 Device	User Name: admin
Manager Version A3(1.0) <sup>host1</sup>	Password: •••••• Login Change Password Help

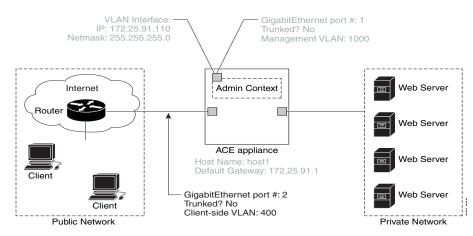
Figure 2-6 Device Manager GUI Login Window

- Step 3 In the User Name field, type **admin** for the admin user account.
- Step 4 In the Password field, type the new password that you entered in Step 2 in "Enabling Management Connectivity Using the Setup Script."
- Step 5 Click Login. The default window that appears is the Virtual Contexts window with the Admin context listed, as shown in Figure 2-7.

#### Figure 2-7 Virtual Contexts Pane (Admin Context)

## **Configuring a Second Gigabit Ethernet Interface Port**

You can configure a second Gigabit Ethernet interface port to connect to clients. For the example configuration, you will configure Gigabit Ethernet interface port 2 as illustrated in Figure 2-8 (previously configured settings are grayed out).



#### Figure 2-8 Configuring a Second Gigabit Ethernet Interface Port to Connect to Clients

Configure a second Gigabit Ethernet port by following these steps:

Step 1 Choose Config > Virtual Contexts > Network > GigabitEthernet Interfaces. The GigabitEthernet Interfaces pane appears (Figure 2-9).



Only users authenticated in the Admin context can configure the Gigabit Ethernet interface ports.

de de	ACE 4710 Device Manage	r A3(1.0)				Welcome admin	Logout + Help
cisco	🖓 Config 🔍 Mor	itor 📑 Admin					
Virtual Contexts + Operations							
System	Config > Virtual Contexts > Net		rnet Interfac	es	_		in the second se
Load Balancing	🗟 🗟 🖉 💽 🤋 Admin	<b>*</b>					
-	ligabitEthernet Interfaces					đ	7 🖬 🕘
Security >	🖓 Interface Name 🍸	Description	Admin Status	Speed	Duplex	Port Operation Mode	FT Vian
	1 gigabitEthernet1/1		Up	Auto	Auto	Switchport	
TOTOLS -	2 gigsbitEthernet1/2		Down	Auto	Auto		
TOTS STREET A NOTIFICAD	3 gigsbitEthernet1/3		Down	Auto	Auto		
argumeetinet anterraces	4 O gigsbitEthemet1/4		Down	Auto	Auto		
BVI Interfaces							
Ratic Routes							
alobal IP DHICP							
tigh Avrailability (HA)							
A Tracking and Failure Detection							
xpert >							

#### Figure 2-9 GigabitEthernet Interfaces Pane—gigabitEthernet 1/2

**Step 2** In the GigabitEthernet Interfaces pane, choose **gigabitEthernet 1/2**, and then click **Edit** to define attributes for the port. The GigabitEthernet Interfaces window appears (Figure 2-10).

Figure 2-10	GigabitEthernet Interfaces	Window—gigabitEthernet 1/2
	e.gaz.i=i.i.i.i.i.i.i.i.i.i.i.i.i.i.i.i.i.i.	<u>g.g.a</u>

	ACE 4710 Dev	ice Manager A3(1.0)	Welcome admin	Logout + Help
cisco	🔩 Carlig	🛃 Monitor 🛛 📑 Admin		
Wrtual Contexts - Operations				
System		Contexts >Network >GigabitEthern	et Interfaces	5
Load Balancing				
59.	- GigabitEthernet Inte			
Security	🖓 Interface Name 🌱	gigabitEthernet1/2		
Network.	Description:	Clent-side		
- Port Channel Interfaces	Admin Status* :	ODD Up ○Down		
- GigabitEthernet Interfaces	Speed* :	Auto 🐱		
<ul> <li>VLAN Interfaces</li> <li>BVI Interfaces</li> </ul>	Duplex* :	O Auto ○ Half ○ Full		
- Static Routes	Port Operation Mode:	O ∧//A O Channel-group ⊙ Switchport		
- Global IP DHCP	Switchport type* :	Access      Trunk		
High Availability (HA)	Access Vian:	400		
HA Tracking and Failure Detection	FT Vian:			
Expert •	Carrier Delay:	0		
	QoS Trust COS:			
		_	Deploy Now Cancel	
< > >				
Ready			V DM in sync with CLI 04-Aug	-2008
NIN Keady			V DH IN SYNC WEN CLT 04-Aug	2008

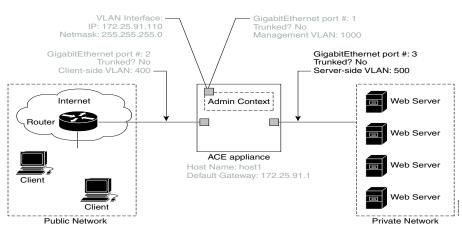
- **Step 3** Enter the following attributes for port 2. Leave the remaining attributes blank or with their default values.
  - Admin Status: Up
  - Speed: Auto
  - Port Operation Mode: Switchport
  - Switchport type: Access
  - Access Vlan: 400
- **Step 4** Click **Deploy Now** to save these settings and to return to the GigabitEthernet Interfaces pane (Figure 2-11).

#### Figure 2-11 GigabitEthernet Interfaces Pane with Ethernet Port 2 Configured

					Edit Bu	
ahaha	ACE 4710 Device Manager				Welcome admin	Logout + He
CISCO	🦓 Contig 🔍 Monit	or 🤄 Admin				
Virtual Contexts 👻 Operation						
ystem	Config > Virtual Contexts > Netw	-	ernet Interfac	es	V	_
ad Balancing						
9.	GigabitEthernet Interfaces				<u></u>	7 - 0
cunty	SInterface Name **	Description	Admin Status	Speed Duple:		FT Vian
twork.	<ul> <li>1 O gigabitEthernet1/1</li> </ul>		Up	Auto Auto	Switchport	
rt Channel Interfaces	2 • gigabitEthernet1/2	Client-side	Up	Auto Auto		
gabitEthernet Interfaces	3 gigabitDhemet1/3		Down	Auto Auto		
AN Interfaces I Interfaces	4 gigabitEthernet1/4		Down	Auto Auto		
atic Routes						
shal IP DHCP						
h Availability (HA)	•					
Tracking and Fallure Detection	•					
pert	•					
Ready					Configurations are in sync 01-Au	- 2008

# **Configuring a Third Gigabit Ethernet Interface Port**

You can configure a third Gigabit Ethernet interface port to connect to the servers. For the example configuration, you will configure Gigabit Ethernet interface port 3 as illustrated in Figure 2-12 (previously configured settings are grayed out.)



# Figure 2-12 Configuring a Third Gigabit Ethernet Interface Port to Connect to the Servers

Configure a third Gigabit Ethernet port by following these steps:

- Step 1 In the GigabitEthernet Interfaces pane, choose gigabitEthernet 1/3, and then click Edit to define attributes for the port. The GigabitEthernet Interfaces window appears (Figure 2-10).
- Step 2 Enter the following attributes for port 3. Leave the remaining attributes blank or with their default values.
  - · Admin Status: Up
  - Speed: Auto
  - · Port Operation Mode: Switchport
  - Switchport type: Access
  - Access VLAN: 500

**Step 3** Click **Deploy Now** to save these settings and to return to the GigabitEthernet Interfaces pane (Figure 2-13).

#### Figure 2-13 GigabitEthernet Interfaces Pane with Ethernet Port 3 Configured

ahaha	ACE 4710 Device Mana				Welcome admin	Logout + He
CISCO	🛛 🗞 Contra 🗋 🍕 M	ionitor 📑 Admin				
Virtual Contexts + Operations						
System	Config > Virtual Contexts > Ne		ernet Interface			_
Load Balancing	Admin	<u>~</u>				
\$9.	GigabitEthernet Interfaces				cí 🗹	I 🝸 🖃 🌚
Security	PInterface Name	Description	Admin Status	Speed Duplex	Port Operation Mode	FT Vian
Network.	<ul> <li>gigabitEthemet1/1</li> </ul>		Up	Auto Auto	Switchport	
Port Channel Interfaces	2 gigsbitEthernet1/2	Client-side	Up	Auto Auto	Switchport	
GigabitEthernet Interfaces	3 • gigabitEthernet1/3	Server-side	Up	Auto Auto	Switchport	
VLAN Interfaces	4 gigsbitEthemet1/4		Down	Auto Auto		
BVI Interfaces						
Static Routes Global IP DHCP						
High Availability (HA)						
HA Tracking and Failure Detection	1					
Expert	-					
Ready	>			<b>V</b> (0	nfigurations are in sync 👔 04-Au	9-2008

# Setting Up an ACE Appliance Using the CLI

You can set up an ACE appliance using the Device Manager GUI or the CLI. This section describes how to set up an ACE using the CLI, and includes the following topics:

- Logging in to the ACE
- Configuring the First Gigabit Ethernet Port
- Allocating the First Gigabit Ethernet Port to a VLAN
- Configuring a Management VLAN Interface on the ACE
- Configuring a Second Gigabit Ethernet Interface Port
- Configuring a Third Gigabit Ethernet Interface Port
- Configuring Remote Management Access to the ACE
- Accessing the ACE through a Telnet Session

# Logging in to the ACE

After you have established a direct serial connection between the ACE and your terminal or a PC (see the "Establishing a Console Connection on the ACE" section), you can set up the ACE using the CLI.

When the setup script displays the "Would you like to enter the basic configuration dialog? (yes/no):" prompt, enter **no** to access the CLI. Log in to the ACE by following these steps:

Step 1 At the login prompt, enter **admin**. For the password, type the new password that you entered in Step 2 in the "Enabling Management Connectivity Using the Setup Script" section.

```
host1 login: admin
Password: xxxxx
```

You are ready to use the ACE CLI when the following prompt appears.

host1/Admin#

Step 2 Set the **terminal session-timeout** command to 0 to prevent this current session from timing out. By default, a session on the ACE is automatically logged out after 5 minutes of inactivity.

```
host1/Admin# terminal session-timeout 0
host1/Admin#
```

#### **Configuring the First Gigabit Ethernet Port**

You can configure a Gigabit Ethernet interface port for the ACE management traffic. For the example configuration, you will configure Gigabit Ethernet interface port 1. Configure the first Gigabit Ethernet port by following theses steps:

Step 1 Configure a Layer 2 Gigabit Ethernet port on the ACE by using the interface gigabitEthernet slot\_number/port\_number command in configuration mode.



**Note** The slot\_number specifies the physical slot on the ACE that contains the Ethernet ports. For the current release of the ACE appliance, this selection is always 1.

Configure Gigabit Ethernet port 1 and enter interface configuration mode by entering:

```
host1/Admin# config
host1/Admin(config)# interface gigabitEthernet 1/1
host1/Admin(config-if)#
```

Step 2 Enable the Gigabit Ethernet port by using the no shutdown command in interface configuration mode. Disable a running Gigabit Ethernet port by using the shutdown command; bring one up by using the no shutdown command.

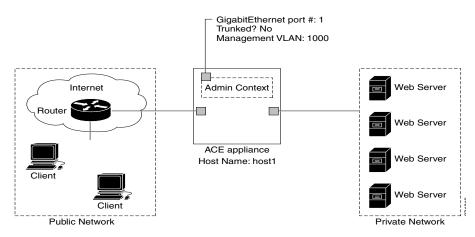
host1/Admin(config-if)# no shutdown

Step 3 Display the configuration of the interface by using the **do** command with the **show** interface command.

host1/admin(config-if)# do show interface vlan 1000

## Allocating the First Gigabit Ethernet Port to a VLAN

After you configure an Gigabit Ethernet port, the next step is to allocate it to a VLAN. For the example configuration, you will allocate the first Gigabit Ethernet port to VLAN 1000, as illustrated in Figure 2-14 (previously configured settings are grayed out.)

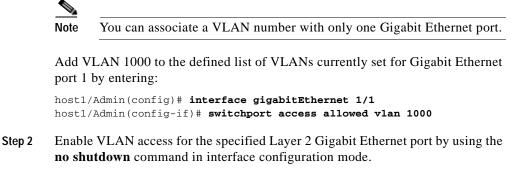


#### Figure 2-14 Allocating the First Gigabit Ethernet Port to a VLAN

Allocate the port to a VLAN by following these steps:

- Step 1 Assign one or more VLAN numbers to the Gigabit Ethernet port by using the switchport trunk allowed vlan *vlan\_list* command in interface configuration mode. The vlan\_list argument can include:
  - A single VLAN number
  - · Beginning and ending VLAN numbers separated by a hyphen
  - Specific VLAN numbers separated by commas

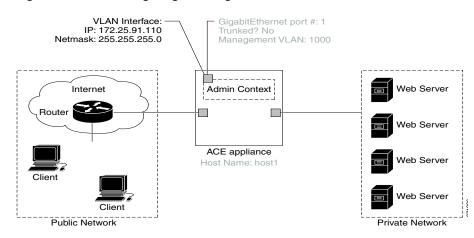
Valid entries are 1 through 4094. Do not enter any spaces in a hyphenated range or in a comma-separated list of numbers in the vlan\_list argument.



```
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
host1/Admin(config)#
```

# Configuring a Management VLAN Interface on the ACE

You can provide management connectivity to the ACE by assigning an IP address to the VLAN interface on the ACE. For the example configuration, you will assign an IP address 172.25.91.110 and a subnet mask of 255.255.255.0 to VLAN 1000, as illustrated in Figure 2-15 (previously configured settings are grayed out).



TH ANT 1000

#### Figure 2-15 Configuring a Management VLAN Interface on the ACE

Configure a VLAN interface on the ACE by following these steps:

1 C 1

• • •

C.

. •

Step 1	Access interface configuration mode for the VLAN 1000.
	host1/Admin(config)# <b>interface vlan 1000</b> host1/Admin(config-if)#
Step 2	Assign an IP address of 172.25.91.110 and a subnet mask of 255.255.255.0 to the VLAN interface for management connectivity.
	host1/Admin(config-if)# ip address 172.25.91.110 255.255.255.0
Step 3	(Optional) Provide a description for the interface. host1/Admin(config-if)# description Management connectivity on VLAN 1000
Step 4	Enable the VLAN interface. host1/Admin(config-if)# <b>no shutdown</b>
Step 5	Display the configuration of VLAN 1000. host1/Admin(config-if)# do show interface vlan 1000

**Step 6** Verify network connectivity by using the **ping** command. This command verifies the connectivity of a remote host or server by sending echo messages from the ACE.

host1/Admin(config-if)# do ping 172.25.91.110

Step 7 Exit the interface configuration mode. host1/Admin(config-if)# exit

host1/Admin(config)#

#### **Configuring a Second Gigabit Ethernet Interface Port**

You can configure a second Gigabit Ethernet interface port to connect to clients. For the example configuration, you will configure Gigabit Ethernet interface port 2 as illustrated in Figure 2-8. Configure the second Gigabit Ethernet Interface port by following these steps:

Step 1 Add VLAN 400 to the defined list of VLANs currently set for Gigabit Ethernet port 2.

host1/Admin(config)# interface gigabitEthernet 1/2 host1/Admin(config-if)# switchport access vlan 400

**Step 2** Enable the Gigabit Ethernet port.

host1/Admin(config-if)# no shutdown host1/Admin(config-if)# exit host1/admin(config)#

# Configuring a Third Gigabit Ethernet Interface Port

You can configure a third Gigabit Ethernet interface port to connect to the servers. For the example configuration, you will configure Gigabit Ethernet interface port 3 as illustrated in Figure 2-12. Configure the third Gigabit Ethernet Interface port by following these steps:

Step 1 Add VLAN 500 to the defined list of VLANs currently set for Gigabit Ethernet port 3.

host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# switchport access allowed vlan 500

**Step 2** Enable the Ethernet port.

host1/Admin(config-if)# no shutdown host1/Admin(config-if)# exit host1/admin(config)#

# **Configuring Remote Management Access to the ACE**

Before remote network access can occur on the ACE through an Ethernet port, you must create a traffic policy that identifies the network management traffic that can be received by the ACE. Configure remote management access to the ACE by following these steps:

- Step 1 Create a management-type class map named REMOTE\_ACCESS that matches
   any traffic.
   host1/Admin(config)# class-map type management match-any REMOTE\_ACCESS
   host1/Admin(config-cmap-mgmt)#
- **Step 2** (Optional) Provide a description for the class map.

host1/Admin(config-cmap-mgmt)# description Remote access traffic match

**Step 3** Configure the match protocol to permit traffic based on the SSH, Telnet, and ICMP protocols for any source address.

```
host1/Admin(config-cmap-mgmt)# match protocol ssh any
host1/Admin(config-cmap-mgmt)# match protocol telnet any
host1/Admin(config-cmap-mgmt)# match protocol icmp any
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

Step 4 Create a REMOTE\_MGMT\_ALLOW\_POLICY policy map for traffic destined to an ACE interface.

host1/Admin(config)# policy-map type management first-match
REMOTE\_MGMT\_ALLOW\_POLICY
host1/Admin(config-pmap-mgmt)#

**Step 5** Apply the previously created REMOTE\_ACCESS class map to this policy.

host1/Admin(config-pmap-mgmt)# class REMOTE\_ACCESS host1/Admin(config-pmap-mgmt-c)#

**Step 6** Allow the ACE to receive the configured class map management protocols.

```
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
host1/Admin(config)#
```

Step 7 Access interface configuration mode for the VLAN to which you want to apply the policy map.

```
host1/Admin(config)# interface vlan 1000
host1/Admin(config-if)#
```

- Step 8 Apply the REMOTE\_MGMT\_ALLOW\_POLICY policy map to the interface. host1/Admin(config-if)# service-policy input REMOTE\_MGMT\_ALLOW\_POLICY
- **Step 9** Display the REMOTE\_MGMT\_ALLOW\_POLICY policy applied to the interface.

```
host1/Admin(config-if)# do show service-policy
REMOTE_MGMT_ALLOW_POLICY
```

Status : ACTIVE
....
Interface: vlan 1000
service-policy: REMOTE\_MGMT\_ALLOW\_POLICY

Step 10 Save your configuration changes from the running configuration to the startup configuration.

host1/Admin(config-if)# do copy running-config startup-config

Generating configuration.... running config of context VC\_web saved

host1/Admin(config-if)# exit
host1/Admin(config)# exit

#### Step 11 Display the running configuration.

host1/Admin(config)# do show running-config Generating configuration.... class-map type management match-any REMOTE\_ACCESS description Remote access traffic match 2 match protocol telnet any 3 match protocol ssh any 4 match protocol icmp any policy-map type management first-match REMOTE\_MGMT\_ALLOW\_POLICY class REMOTE\_ACCESS permit interface vlan 1000 description Management connectivity on VLAN 1000 ip address 172.25.91.110 255.255.255.0 service-policy input REMOTE\_MGMT\_ALLOW\_POLICY no shutdown interface vlan 400 description client connectivity on VLAN 400 ip address 10.10.40.10 255.255.255.0 no shutdown

# Accessing the ACE through a Telnet Session

After you have completed the previous configurations, you can use Telnet to access the ACE through an Ethernet port by using its IP address. Access the ACE through Telnet by following these steps:

Step 1 Initiate a Telnet session from a remote host to the ACE. For example, access the ACE from the VLAN IP address of 172.25.91.110 by entering:

remote\_host# telnet 172.25.91.110

Trying 172.25.91.110... Open

Step 2 At the prompt, log in to the ACE. Enter **admin** as the user name and for the password, type the new password that you entered in the Step 2 in "Enabling Management Connectivity Using the Setup Script" section.

host1 login: **admin** Password: **xxxxx** 

Step 3 Display the Telnet session.

In this chapter, you have set up your ACE appliance so that you can use the ACE Device Manager or CLI to perform server load-balancing configuration tasks through a remote management interface. Next, you will create a user context for server load balancing.



# CHAPTER **3**

# **Creating a Virtual Context**

This chapter describes how to create a virtual context for the Cisco 4700 Series Application Control Engine (ACE) appliance.

This chapter contains the following sections:

- Overview
- Creating a Virtual Context Using the Device Manager GUI
- Creating a Virtual Context Using the CLI

# **Overview**

After reading this chapter, you should have a basic understanding of ACE appliance virtualization and be able to partition your ACE into multiple virtual devices or virtual contexts (VCs) for more efficient operation.

Virtualization allows you to create a virtual environment in which a single ACE is partitioned into multiple virtual devices, each functioning as an independent ACE appliance that is configured and managed independently.

You set up virtualization by performing the following configuration steps:

- Configure resource allocation for a virtual context
- Create a virtual context
- Configure access to the virtual context

An example virtual environment will be used throughout this guide, with the user context VC\_web, for the web traffic through the network. This user context will be associated with the custom resource class RS\_web.

In this chapter, you will create a virtual context. In subsequent chapters, you will create a virtual server within the virtual context. The virtual server is associated with a server farm and real servers. The example setup is illustrated in Table 3-1.

Virtual Context	Virtual Server	Server Farm	Real Servers
VC mak			RS_web1
	VS web	SF web	RS_web2
VC_web	vs_web	Sr_web	RS_web3
			RS_web4

Table 3-1 Example Virtual Contexts

Before you begin configuring your ACE for virtualization, you should become familiar with a few concepts: virtual context, Admin and user contexts, and resource classes.

With ACE virtualization, you can create a virtual environment, called a virtual context, in which a single ACE appears as multiple virtual devices, each configured and managed independently. A virtual context allows you to closely and efficiently manage system resources, ACE users, and the services that you provide to your customers.

By default, the ACE initially provides you an Admin context, with the ability to define up to five user contexts. (With additional licenses, you can define up to 20 contexts.)

As the system administrator, you have full system administrator access to configure and manage the Admin context and all user contexts. Each context can also have its own administrator and log-in mechanism that provides access only to the specific context. When you log in to the ACE using the console or Telnet, you are authenticated in the Admin context.

Although virtualization allows you to create multiple contexts, in the physical world, you still have a single ACE with finite resources, such as the number of concurrent connections. To address this limitation, the ACE provides resource classes that allow you to manage each virtual context's access to physical ACE

resources. A resource class is a definition of what portion of an ACE's overall resources will be assigned, at a minimum or maximum, to any given context. One resource class may be associated with one or more contexts.

The ACE is preconfigured with a default resource class for the Admin context. This default resource class is applied to all virtual contexts that you create. It allows a maximum of 100 percent access to all resources by all virtual contexts. When a resource is being used to its maximum limit, the ACE will deny additional requests for that resource from any other virtual contexts. To avoid oversubscribing resources and to help guarantee that resource availability is shared among multiple virtual contexts, you create custom resource classes and associate them with the virtual contexts you define.

# Creating a Virtual Context Using the Device Manager GUI

This section describes how to create and configure a virtual context for server load balancing using the ACE Device Manager user interface and contains the following topics:

- Creating a Resource Class
- Creating a Virtual Context
- Configuring the Client-Side VLAN Interface
- Configuring the Server-Side VLAN Interface

### **Creating a Resource Class**

Create a resource class by following these steps:

Step 1 Choose Config > Virtual Contexts > System > Resource Class. The Resource Classes pane appears.

Figure 3-1 Resource Classes Pane

				Add Button	
cisco	ACE 4710 Device	Manager A3(1.0)		Welcome av min	Logout + Help
Wrbual Contexts 👻 Operations					
System		ts >System >Resource Cla	15		0
- Primary Attributes	🔹 🔍 🖉 🕞 🤋 Admin	×		¥	
- Syslog	Resource Classes			• C 5	9 🛛 🖓 🖬
<ul> <li>SMMP</li> <li>Global Policy</li> </ul>	Name		firtual Context	Maximum VC	
- Licenses	1 O default	1		N/A	
- Resource Class					
<ul> <li>Application Acceleration and Optimization</li> </ul>					
Load Balancing					
53.					
Security					
Network.					
High Availability (HA) HA Tracking and Falure Detection					
Expert					
<			V	Configurations are in sync 04-Ac	(Sortinits @-2008

Step 2 Click Add. The New Resource Class window appears (Figure 3-2).

#### ACE 4710 Device Manager A3(1.0) Welcome admin Logout + Help ահահո Monitor Admin 🦓 Contig CISCO Virtual Contexts Operations Config >Virtual Contexts >System >Resource Class >Add System C 🕑 ? Admin ~ da. Primary Attributes New Resource Class Syslog - SMP Name\* : R.C\_web Global Policy Al\* : O Default Min: 0.0 % Max: Unlimited ¥ Licenses Acc-Connections : Operault OMn: % Macc Equal to Min 🖂 Resource Class Application Acceleration and Optimization ACL-Memory: Obefault O Min: % Max: Equal to Min 💌 Load Balancing Conc-Connections: Opefault OMin: % Marc Equal to Min 🖂 5SL ) HTTP-Comp: Operault OMn: % Max: Equal to Min Security Mgnit-Connections: Operault OMn: % Max: Equal to Min 🖂 Network Proxy-Connections: Opefault OMin: % Marc Equal to Min High Availability (HA) Regexp: Operault OMin: % Max: Equal to Min M HA Tracking and Failure Detection Sticky: Obefault OMin: % Mac: Equal to Min 🕑 Expert xlates: ODefault ○Min: % Marc Equal to Min Buffer-Syslog: Operault O Min: % Mate Equal to Min IV Rate-Inspect-Conn: Obefault OMn: % Mac: Equal to Min 🕑 Rate-Bandwidth: Obefault OMn: % Marc Equal to Min Rate-Connections: Obefault OMin: % Max: Equal to Min | v Rate-Mgmt-Traffic: Obefault OMn: % Marc Equal to Min Rate-SSL-Connections: Operault O Min: % Marc Equal to Min 🗸 Rate-Syslog: Obefault O Min: % Max: Equal to Min M Rate-MAC-Miss: Opefault O Min: % Matc Equal to Min 19 Deploy Now 271862 Ready V DM in sync with CLI 04-Aug-2008

#### Figure 3-2 New Resource Class Window

- **Step 3** Enter the following Resource Class attributes. Leave the remaining attributes blank or with their default values.
  - Name: RC\_web
  - Default Min: 10
  - Default Max: Unlimited
- **Step 4** Click **Deploy Now**. The Resource Classes pane appears with the newly added resource class (Figure 3-3).

#### Figure 3-3 Resource Classes Pane with a New Resource Class Added

cisco	ACE 4710 Devic	e Manager A3( <sup>,</sup>	1.0)	Welcome admin	Logout + Help
Virtual Contexts 👻 Operations					
System - Primary Attributes - Syskog	4 • • • • • A		m >Resource Class		0
SNMP Global Policy Ucenses Resource Class Replication Acceleration and Optimization Load Balancing SSL Security High Availability (14) HA Tracking and Falure Detection Expert	Resource Classes Name 1 OdefauR 2 ORC_web	* 1 1	# Virtual Context		inum VC
					Virtual Contexts
A Ready				Configurations are in sync	

Ţ

# **Creating a Virtual Context**

You can create a user context for server load-balancing purposes. For the example configuration, you will create a user context, VC\_web, and configure a management VLAN interface to VLAN 1000, as illustrated in Figure 3-4 (previously configured settings are grayed out).

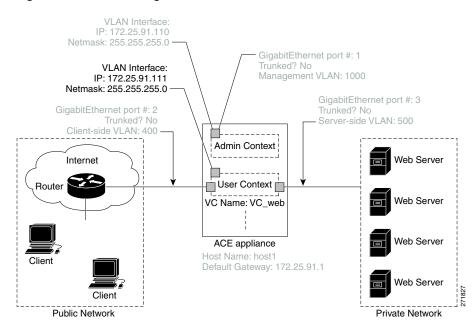


Figure 3-4 Creating a User Context

Create a virtual context by following these steps:

Step 1 Choose Config > Virtual Contexts. The All Virtual Contexts pane appears (Figure 3-5).



de de	ACE 4710	Device Manag	er A3(1.0)			Welcome	admin	Logout + Help
cisco	🗐 🖓 Cor	fia 🛛 🔍 Mar	itor 📑 Admin					
Virtual Contexts - Operations	-							
System	Config >Virt	ual Contexts	_	_	_	_	_	9
Load Balancing								
551.	All Virtual Conti						• 6	3 7 🖻
Security	Name	Resource Class	Management IPs	Config Status	HA State	HA Peer State	HA Peer	HA Autosync
Network	1 O Admin	default	172.25.91.41	V OK	A)/A	∆¦A		brue
High Availability (HA)	•							
HA Tracking and Failure Detection								
Expert	•							

Step 2 Click Add. The New Virtual Context window appears (Figure 3-6).

ahaha	ACE 4710 D	evice Manager A3	Welcome admin	Logout + Help	
CISCO	🗐 🐴 Config	Monitor	Ramin		
Virtual Contexts    Operations					
System +	Config >Virtual Co	ntexts∋Add	_		0
Load Balancing	- New Virtual Context				
59.	Name* :	VC_web			
Security +	Resource Class* ;		a a constant		
Network.	Alocate-Interface VLANs* :	110,400,500	nn.		
High Availability (HA)	Description:				
HA Tracking and Failure Detection	Description.	Virtual context for marke	eting web site		<u>_</u>
Expert +					
					*
	Policy Name* :	managemenk			
	VLANs to Use* :	110			
	Management IP* :	172.25.91.111			
	Management Netmask* :	255.255.255.0 💌			
	Protocols to Allow* :		lected Items		
	Default Gateway IP:	172.25.91.1			
	SMMP v2c Community:	public			
		Community string re-	quired for monitoring virtual co	antexta.	
<u>c</u>				Deploy Now	Cancel [8]
Ready				Configurations are in sync 04-Aug-20	32

#### Figure 3-6 New Virtual Context Window

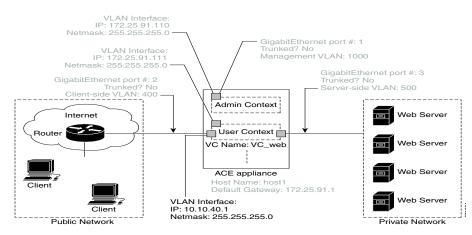
- **Step 3** Enter the following virtual context attributes. Leave the remaining attributes blank or with their default values.
  - Name: VC\_web
  - Resource Class: RC\_web
  - Allocate-Interface VLANs: 1000, 400, 500 (these VLANs allow the context to receive the associated traffic)
  - · Description: Virtual context for marketing website
  - Policy Name: Management

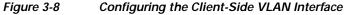
- VLANs to Use: 1000 (this VLAN allows for remote management of the context)
- Management IP: 172.25.91.111 (this IP address also allows for remote management of the context)
- Management Netmask: 255.255.255.0
- Protocols to Allow: SNMP (or any protocols that you allow for this virtual context)
- Default Gateway IP: 172.25.91.1
- **Step 4** Click **Deploy Now** to deploy this context. Then, choose **Virtual Contexts**. The window refreshes with the new virtual context listed in the All Virtual Contexts pane (Figure 3-7).

#### Figure 3-7 All Virtual Contexts Pane After VC\_web is Added

# Configuring the Client-Side VLAN Interface

You can now configure a client-side VLAN interface, which is the address to which client traffic is sent. For the example configuration, you will configure VLAN 400 (Figure 3-8).





Configure a client-side VLAN interface by following these steps:

- Step 1 Choose VC\_web in the virtual contexts drop-down list.
- Step 2 Choose Config > Virtual Contexts > Network > VLAN Interfaces. The VLAN Interfaces pane appears (Figure 3-9).

L

#### ACE 4710 Device Manager A3(1.0) Welcome admin Logout + Help ահանո 🦓 Carla CISCO Monitor Canal Admin Virtual Contexts + Operations Config Virtual Contexts >Network >VLAN Interfaces System . 🔹 🔍 🖉 🕞 🤋 VC\_web ~ Load Balancing **VLAN Interfaces** \* 6 3 7 8 9 59. **PVLAN** IP Address Description Netmask Admin Status Security 1 💿 110 172.25.91.111 255.255.255.0 Up Network. Port Channel Interfaces GgabitEthernet Interfaces VLAN Interfaces BVI Interfaces Static Routes - Global IP DHCP High Availability (HA) HA Tracking and Failure Detection Expert Policy Access Group Static ARP Entries NAT Pool DHCP Relay Configuration Policy @ 110 • 3 7 H • Policy Map Direction 1 📀 management input 1887 271 Ready ✓ Configurations are in sync 04-Aug-2008

#### Figure 3-9 VLAN Interfaces Pane

Step 3 Click Add to add a new VLAN interface. The VLAN Interfaces window appears (Figure 3-10).

#### Figure 3-10 VLAN Interfaces Window—VLAN 400

ahaha	ACE 4710 Device	Manager A3(1.0)	Welcome admin Logo		
CISCO	😽 Cortia	🛃 Monitor 🛛 📑 Admin			
Virtual Contents 🐱 Operation	ns				
System		ts>Network>VLAN Interfaces		9	
Load Balancing		×			
59.	VLAN Interfaces				
Security	PVLAN *	400			
Network	Description:	Client side VLAN interface		~	
<ul> <li>Port Channel Interfaces</li> </ul>					
<ul> <li>GgabitEthernet Interfaces</li> </ul>				2	
- YLAN Interfaces	IP Address:	10.10.40.10			
<ul> <li>BVI Interfaces</li> </ul>	Alas IP Address:				
<ul> <li>Static Routes</li> <li>Global IP DHCP</li> </ul>	Peer IP Address:				
High Availability (HA)					
HA Tracking and Falure Detection	- Netronase:	255.255.255.0			
	Admin Stabus* :	⊙Up ©Down			
Expert	ARP Inspection Type:	⊙ A//A ○ Flood ○ No-Flood			
	Max Pragment Chains Allowed:				
	Min MTU Value:				
	Reassembly Timeout:				
	Reverse Path Forwarding (RPF):				
	Bridge Group Number:				
	Enable MAC Address Autogenerate:				
	Enable MAC Sticky:				
	Enable ICMP Guard:				
	Enable DHOP Relay:				
	Enable Normalization:				
	Action for DF BR* :	Allow      Clear			
	Action for IP Header Options:	×			
	Min TTL IP Header Value:				
	Enable Syn Cookie Threshold Value:				
	UDP Config Commands:	N∕⁄A ○IP-Destination-Hash ○IP-Source-Hash			
<	>		Deploy Now Ca	ncel 🔽	
Ready			Configurations are in sync 04-Au	ug-2008	

- **Step 4** Enter the following VLAN attributes. Leave the remaining attributes blank or with their default values.
  - VLAN: 400
  - Description: Client-side VLAN interface
  - IP Address: 10.10.40.10
  - Netmask: 255.255.255.0
  - Admin Status: Up

Step 5 Click Deploy Now at the bottom of the window to save your entry. Then, choose VLAN Interfaces to return to the VLAN Interfaces pane (Figure 3-11).



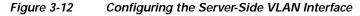
ahaha		ACE 4710 Devic	e Manager A3			Welcome admin	Logout + Help			
CISCO		🔧 Config	Monitor	Admin 💽						
Virtual Contexts   Operation	_		at a blick search							
System	) Loni			VLAN Interfaces			0			
Load Balancing	,									
59.	VLAN I	VLAN Interfaces 🔹 🖬 🖬 🖬 🖗 🚮								
Security		🖓 VLAN 👻	De	scription	IP Address	Netmask	Admin Status			
Network.	+ 1 0	) 110			172.25.91.1		Up			
<ul> <li>Port Channel Interfaces</li> </ul>	2 (	) 400 CI	ient side VLAN interf	sce.	10.10.40	1 255.255.255.0	Up			
<ul> <li>GigabitEthernet Interfaces</li> </ul>										
VLAN Interfaces     UVI Interfaces										
- Static Routes										
- Global IP DHICP										
High Availability (HA)										
HA Tracking and Failure Detection										
Expert										
	Policy		RP Entries NAT Po	ol DHCP Relay Configuration	1					
	Policy	# 110					• 3 V P			
				Policy Map		9Direction				
	1 🤆	)	mar	agement	input					
<	>									
Ready						Configurations are in sync	04-Aug-2008			

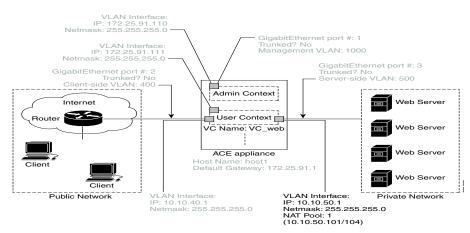
# Configuring the Server-Side VLAN Interface

At this point, you can now configure the server-side VLAN interface, which is the address to which traffic is sent. For the example configuration, you will configure VLAN 500 and a NAT pool for the VLAN (Figure 3-12).



Network Address Translation (NAT) is designed to simplify and conserve IP addresses. It allows private IP networks that use unregistered IP addresses to connect to the Internet. You configure a NAT pool for the ACE so that the ACE exposes only one address for the entire network to the outside world. This pool, which hides the entire internal network behind that address, offers both security and address conservation.

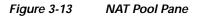




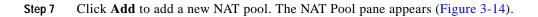
Configure the VLAN interface by following these steps:

- Step 1 Make sure that VC\_web is selected in the virtual contexts drop-down list.
- Step 2 Choose Config > Virtual Contexts > Network > VLAN Interfaces. The VLAN Interfaces pane appears (Figure 3-11).
- Step 3 Click Add to add a new VLAN interface. The VLAN Interfaces window appears (Figure 3-10).

- **Step 4** Enter the following VLAN attributes. Leave the remaining attributes blank or with their default values.
  - VLAN: 500
  - Description: Server-side VLAN interface
  - IP Address: 10.10.50.1
  - Netmask: 255.255.255.0
  - Admin Status: Up
- Step 5Click Deploy Now at the bottom of the window to save your entry. Then, choose<br/>VLAN Interfaces to return to the VLAN Interfaces pane.
- Step 6 Choose the row for VLAN 500, and then choose the NAT Pool tab. The NAT Pool pane appears (Figure 3-13).



ahaha	A	CE 4710 Devic	e Manager A3(1.0)		Welcome admin	Logout + Hel
CISCO		🦓 Conto	🍇 Monitor 🛛 🗟 Admin			
Virtual Contexts   Operations		· .				
System )			exts>Network>VLAN Inte	rfaces		1
Load Balancing		9 %_m	6 <u>v</u>			
S9. D	VLAN Inter	faces			🔹 🖬 🖻	7 🖻 🤤 🔂
Security )	•	🖓 VLAN 👻	Description	IP Address	Netmask.	Admin Status
Vetwork.		110		172.25.91.111	255.255.255.0	Up
Port Channel Interfaces	2 ()	400 C	lent side VLAN interface	10.10.40.1	255.255.255.0	Up
SigabitEthernet Interfaces	3 🕟	500 Se	erver side VLAN interface	10.10.50.1	255.255.255.0	Up
Jobal IP DHCP						
A Tracking and Failure Detection	<u>}</u>					
HA Tracking and Failure Detection	Palay Au		89 Ennes NAT Peal CHCP Relay	Configuration		
HA Tracking and Failure Detection	Policy Ac	500			Manuf	
High Availability (HA)	the second second		89 Ennes NAT Peel BHCP Relay	Configuration End IP Address No records	Netmask.	PAT Enabled
HA Tracking and Failure Detection	the second second	500		End IP Address	Netmask.	



L

#### Figure 3-14 Configuring a NAT Pool

cisco		4710 Device Manager			Welcome admin	Logout + H
Wrtual Contexts + Operatio	ro					
System		tual Contexts >Netwo		15		_
Load Balancing	,	2 VC_web 💌				
59.	VLAN Interface	15			🗠 🗹 🖻	
Security		LAN *	Description	IP Address	Netmask.	Admin Status
Network.	1 0	110		172.25.91.11		
Port Channel Interfaces	2 ()	400 Client side VLAN in		10.10.40.		
GigabitEthernet Interfaces	3 📀	500 Server side VLAN i	nterface	10.10.50.	255.255.255.0	) Up
VLAN Interfaces						
BVI Interfaces						
Static Routes						
Global IP DHCP						
High Availability (HA)						
HA Tracking and Failure Detection						
Expert						
	Poley Arress 9 • NAT Pool # 500 * NAT I'ad # * Start IP Address End IP Address: Netmask* 1 PAT Enabled:	1	T Peal	where T		
					Deploy Now	Cancel 🔀
Ready					✔ Configurations are in sync	

- **Step 8** Enter the following NAT pool attributes. Leave the remaining attributes blank or with their default values.
  - NAT Id: 1
  - Start IP Address: 10.10.50.101
  - End IP Address: 10.10.50.104
  - Netmask: 255.255.255.0

Step 9 Click **Deploy Now** at the bottom of the window to save your entry and return to the NAT Pool pane (Figure 3-15).

#### Figure 3-15 NAT Pool Pane with a NAT Pool Configured

ahaha	ACE 4710 Device	e Manager A3(1.0)		Welcome admin	Logout + He
CISCO	🛛 🐴 Config	💐 Monitor 🛛 🔯 Admin			
Virtual Contexts + Operations					
System 🕨		xts⇒Network⇒VLAN Interface	15		
Load Balancing 🔹 🕨	🌢 🖉 Ø 🕘 ? Wmeb	×			
SSL 🕨	VLAN Interfaces			🖻 🖻 🖻	7 - 9 5
iecurity 🕨	9 VLAN **	Description	IP Address	Netmask.	Admin Status
ietwork. 👻	1 0 110		172.25.91.111	255.255.255.0	Up
ort Channel Interfaces	V	nt side VLAN interface	10.10.40.1	255.255.255.0	Up
igabitEthernet Interfaces	3 📀 500 Ser	ver side VLAN interface	10.10.50.1	255.255.255.0	Up
LAN Interfaces					
VI Interfaces					
tatic Routes					
obal IP DHOP					
igh Availability (HA)					
A Tracking and Failure Detection					
Dipert					
	Pulicy Acress Group Static AR	P Ennes NAT Peel DHCP Relay Configu	uton.		
	Pulky Arress Group State AM	P Entres NAT Peol CHCP Relay Configu	vina )		
	The second se	P Ennes NAT Peel CHCP Relay Configu Start IP Address	ution End 3P Address	Netmask	PAT Enabled
	NAT Pool @ 500				
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	
opert ▶	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	PAT Enabled
	NAT Pool @ 500 ØNAT Id	ØStart IP Address	End IP Address	Netmask.	

# **Creating a Virtual Context Using the CLI**

You can create a virtual context using the command-line interface. This section contains the following topics:

- Configuring a Resource Class
- Creating a Virtual Context
- Configuring a Management VLAN Interface to the User Context
- Configuring Remote Management Access to the User Contexts
- Configuring the Client-Side VLAN Interface
- Configuring the Server-Side VLAN Interface

### **Configuring a Resource Class**

Configure a resource class by following these steps:

Step 1 Using the console, log in to the ACE as the system administrator. For example, enter the following command at a command prompt.

#### Telnet 172.25.91.110

At the prompt, enter **admin**, then the new password you entered in Step 2 in "Enabling Management Connectivity Using the Setup Script" in Chapter 2.

host1 login: **admin** Password: **xxxxx** 

Step 2 Enter configuration mode.

host1/Admin# config
host1/Admin(config)#

**Step 3** Configure a resource class to limit the resources of a context to 10 percent of the total resources available on the ACE, and exit configuration mode.

```
host1/Admin(config)# resource-class RS_web
host1/Admin(config-resource)# limit-resource all minimum 10 maximum
unlimited
host1/Admin(config-resource)# exit
host1/Admin(config)#
```

### **Creating a Virtual Context**

Create a virtual context by following these steps:

```
Step 1 Create a new context.
host1/Admin(config)# context VC_web
```

host1/Admin(config-context)#

**Step 2** Associate three existing VLANs with the context so that the context can receive traffic classified for it.

host1/Admin(config-context)# allocate-interface vlan 1000 host1/Admin(config-context)# allocate-interface vlan 400 host1/Admin(config-context)# allocate-interface vlan 500

Step 3 Associate the context with the resource class that you created in the previous section, "Configuring a Resource Class."

host1/Admin(config-context)# member RC\_web

Step 4 Change to the VC\_web context that you created in Step 1 and exit configuration mode.

host1/Admin(config-context)# do changeto VC\_web
host1/VC\_web(config)# exit
host1/VC\_web#

Step 5 Display the virtual context configuration.

host1/VC\_web# show running-config context

Step 6 Display the resource class configuration. host1/VC\_web# show running-config resource-class

### Configuring a Management VLAN Interface to the User Context

You can provide management connectivity to the user context by assigning an IP address to the VLAN interface, as illustrated in Figure 3-4. Configure a management VLAN interface by following these steps:

Step 1 Access interface configuration mode for VC\_web for the VLAN 1000 on VC\_web.

host1/VC\_web# config host1/VC\_web(config)# interface vlan 1000 host1/VC\_web(config -if)#

Step 2 Assign an IP address of 172.25.91.111 and a subnet mask of 255.255.255.0 to the VLAN interface for management connectivity.

host1/VC\_web(config-if)# ip address 172.25.91.111 255.255.255.0

**Step 3** Enable the VLAN interface.

host1/VC\_web(config-if)# no shutdown

### Step 4 Show that VLAN 1000 is active. host1/VC\_web(config-if)# do show interface vlan 1000

- Step 5 Verify network connectivity. host1/VC\_web(config-if)# do ping 172.25.91.111
- Step 6 Display the ARP table.

**Note** The Address Resolution Protocol (ARP) allows the ACE to manage and learn the mapping of IP to Media Access Control (MAC) information to forward and transmit packets.

host1/VC\_web(config-if) # do show arp

#### Step 7 Exit configuration mode.

host1/VC\_web(config-if)# exit
host1/VC\_web(config)# exit
host1/VC\_web#

### **Configuring Remote Management Access to the User Contexts**

Before remote network access can occur on the user context through an Ethernet port, you must create a traffic policy that identifies the network management traffic that can be received by the ACE. Configure remote management access by following these steps:

Step 1 Create a management type class map named REMOTE\_ACCESS that matches any traffic.

host1/VC\_web# config host1/VC\_web(config)# class-map type management match-any REMOTE\_ACCESS host1/VC\_web(config-cmap-mgmt)#

**Step 2** (Optional) Provide a description for the class map.

```
host1/VC_web(config-cmap-mgmt)# description Remote access traffic
match
```

Step 3 Configure the match protocol to permit traffic based on the SSH, Telnet, and ICMP protocols for any source address.

host1/VC\_web(config-cmap-mgmt)# match protocol ssh any host1/VC\_web(config-cmap-mgmt)# match protocol telnet any host1/VC\_web(config-cmap-mgmt)# match protocol icmp any host1/VC\_web(config-cmap-mgmt)# exit host1/VC\_web(config)#

Step 4 Create a REMOTE\_MGMT\_ALLOW\_POLICY policy map for traffic destined to an ACE interface.

host1/VC\_web(config)# policy-map type management first-match
REMOTE\_MGMT\_ALLOW\_POLICY
host1/VC\_web(config-pmap-mgmt)#

**Step 5** Apply the REMOTE\_ACCESS class map to this policy.

host1/VC\_web(config-pmap-mgmt)# class REMOTE\_ACCESS host1/VC\_web(config-pmap-mgmt-c)# **Step 6** Allow the ACE to receive the configured class map management protocols.

```
host1/VC_web(config-pmap-mgmt-c)# permit
host1/VC_web(config-pmap-mgmt-c)# exit
host1/VC_web(config-pmap-mgmt)# exit
host1/VC_web(config)#
```

Step 7 Access interface configuration mode for the VLAN to which you want to apply the policy map.

```
host1/VC_web(config)# interface vlan 1000
host1/VC_web(config-if)#
```

**Step 8** Apply the REMOTE\_MGMT\_ALLOW\_POLICY policy map to the interface.

host1/VC\_web(config-if)# service-policy input REMOTE\_MGMT\_ALLOW\_POLICY

Step 9 Display the REMOTE\_MGMT\_ALLOW\_POLICY policy applied to the interface.

host1/VC\_web(config-if)# do show service-policy
REMOTE\_MGMT\_ALLOW\_POLICY

Step 10 Copy your configuration changes from the running configuration to the startup configuration.

host1/VC\_web(config-if)# do copy running-config startup-config

Generating configuration.... running config of context VC\_web saved

host1/VC\_web(config-if)# exit
host1/VC\_web(config)# exit

Step 11 Display the running configuration.

host1/VC\_web(config)# do show running-config

### Configuring the Client-Side VLAN Interface

At this point, you can configure a client-side VLAN interface, the address to which the client traffic is sent, as illustrated in Figure 3-8. Configure a client-side VLAN interface by following these steps:

Step 1	Access interface configuration mode for the VLAN 400.
	host1/VC_web(config)# <b>interface vlan 400</b> host1/VC_web(config -if)#
Step 2	Assign an IP address of 10.10.40.1 and a subnet mask of 255.255.255.0 to the VLAN interface for client connectivity. host1/VC_web(config-if)# <b>ip address 10.10.40.1 255.255.255.0</b>
Step 3	(Optional) Provide a description for the interface. host1/VC_web(config-if)# description Client connectivity on VLAN 400
Step 4	Enable the VLAN interface. host1/VC_web(config-if)# <b>no shutdown</b>
Step 5	Show that VLAN 400 is active. host1/VC_web(config-if)# <b>do show interface vlan 400</b>
Step 6	Display the ARP table. host1/VC_web(config-if)# <b>do show arp</b>
Step 7	Exit configuration mode. host1/VC_web(config-if)# exit host1/VC_web(config)# exit

host1/VC\_web#

### Configuring the Server-Side VLAN Interface

Next, you can configure a server-side VLAN interface, the address to which the server traffic is sent, as illustrated in Figure 3-12. Configure the server-side VLAN interface by following these steps:

Step 1	Access interface configuration mode for the VLAN 500.
	<pre>host1/VC_web# config host1/VC_web(config)# interface vlan 500 host1/VC_web(config -if)#</pre>
Step 2	Assign an IP address of 10.10.50.1 and a subnet mask of 255.255.255.0 to the VLAN interface for server-side connectivity.
	<pre>host1/VC_web(config-if)# ip address 10.10.50.1 255.255.255.0</pre>
Step 3	(Optional) Provide a description for the interface.
	<pre>host1/VC_web(config-if)# description Server connectivity on VLAN 500</pre>
<b>.</b>	Enable the VLAN interface.
Step 4	
Step 4	<pre>host1/VC_web(config-if)# no shutdown</pre>
Step 4 Step 5	host1/VC_web(config-if)# <b>no shutdown</b> Configure a NAT pool.
•	
	Configure a NAT pool. host1/VC_web(config-if)# nat-pool 1 10.10.50.101 10.10.50.104 netmask
Step 5	Configure a NAT pool. host1/VC_web(config-if)# nat-pool 1 10.10.50.101 10.10.50.104 netmask 255.255.255.0
Step 5	Configure a NAT pool. host1/VC_web(config-if)# nat-pool 1 10.10.50.101 10.10.50.104 netmask 255.255.255.0 Show that VLAN 500 is active.
Step 5 Step 6	Configure a NAT pool. host1/VC_web(config-if) # nat-pool 1 10.10.50.101 10.10.50.104 netmask 255.255.255.0 Show that VLAN 500 is active. host1/VC_web(config-if) # do show interface vlan 500
Step 5 Step 6	Configure a NAT pool. host1/VC_web(config-if) # nat-pool 1 10.10.50.101 10.10.50.104 netmask 255.255.255.0 Show that VLAN 500 is active. host1/VC_web(config-if) # do show interface vlan 500 Display the ARP table.

In this chapter, you have partitioned your ACE into an Admin context and a user context VC\_web. Each of the virtual contexts is now associated with a resource class that is appropriate to its intended use. You have also configured a management VLAN interface, as well as the client and server VLAN interfaces to the user context.

In the next chapter, you will configure an access control list to secure your network.





# **Configuring Access Control Lists**

This chapter describes how to configure access control lists (ACLs) for the Cisco 4700 Series Application Control Engine (ACE) appliance. This chapter contains the following sections:

- Overview
- Configuring an ACL Using the Device Manager GUI
- Configuring an ACL Using the CLI

### **Overview**

After reading this chapter, 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 4700 Application Control Engine 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:

- Step 1 Choose VC\_web.
- Step 2 Choose Config > Virtual Contexts > Security > ACLs. The ACLs pane appears, listing the existing ACLs (Figure 4-1).

#### Figure 4-1 ACLs Pane

ahaha	ACE 4710 Device				Welcome admin	Logout • Help
CISCO	🗧 🦓 Contig	🔍 Monitor	la Admin			
Wrtual Contexts   • Operations						
System •	Config > Virtual Co					D
Load Balancing	* • • • • ? w	C_web 🛛	1			
551. •	ACLS				•	I 🔽 🖦 🚮
Security		Nome		Туре	Remark	
ACLS				No recorde		
- Object Groups	1					
Network.						
High Availability (HA)						
HA Tracking and Failure Detection						
Expert						
					Res Construction	10120000
×					Res (	ensense

# Step 3 Click Add to create an ACL. The ACL configuration window appears (Figure 4-2).

#### Figure 4-2 ACL Configuration Window

ahaha	ACE 4710 Device Manager A3(1.0)	Welcome admin	Logout + Help
CISCO	🗏 🦓 Config 🔣 Monitor 🔄 🧟 Admin		
Virtual Contexts 👻 Operations			
System	Config >Virtual Contexts >Security >ACLs		line in the second s
Load Balancing	🔷 🔍 🕐 🤋 Wmb  💌		
59.	ACLS		
Security	VName*: ACL_permit_al		
- ACLS	Type*:  • Extended  • EtherType		
- Object Groups	Remark:		
Network	→	Deploy Now Car	ncel 🔊
High Availability (HA)	<b>&gt;</b>		
HA Tracking and Failure Detection	•		
Expert	•		
<u>&lt;</u>	<u>x</u>		up-2008
Ready		Configurations are in sync 01-Au	ig-2008

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

Step 6 Click Add to create an ACL entry. The ACL entry configuration window appears (Figure 4-3).

1.1	ACE 4710 Device Ma	inager A3(1.0)		Welcome admin	Logout	<ul> <li>Help</li> </ul>
cisco	🦓 Contia 🛛 🧕	Monitor 📑 Admin				
Virtual Contexts   Operations						
System	Config >Virtual Conte	-		_	_	<b>D</b>
Load Balancing	* • • • • ? VC_web	× •				
59.						
Security						
- ACLS	Type*: ①Extended 〇E	therType:				_
- Object Groups	Remark					
Network.	1		Deploy Nov	Cancel	Delete	
High Availability (HA)	Faturdad					
HA Tracking and Failure Detection	Extended @ ACL_permit_all -					5
Expert	\$ \$\$Line No.* :	1				
	Permit:	<b>v</b>				
	Service object group:	⊙ N/A				
	Protocol* :	IP (Any)				
	Source Network object group:	⊙ N/A				
	Any Source:					
	Destination Network object group:					
	Any Destination:					
				Deploy Now	Cancel 💦	
< >						
Ready			✓ Conf	igurations are in sync	04-Aug-2008	

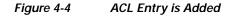
#### Figure 4-3 ACL Entry Configuration Window

- **Step 7** Create an ACL entry with the following attributes. Leave the remaining attributes blank or with the default values.
  - Line No.: 1

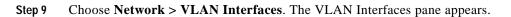


For easier insertion of additional ACL entries later, you can enter non-sequential line numbers such as 10, 20, and so on.

- Permit: (Checked)
- Protocol: IP (Any)
- Any Source: (Checked)
- Any Destination: (Checked)
- **Step 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 4-4).



ahaha	ACE 4710 Device Manager A3(1.0)	Welcome admin	Logout • Help
CISCO	🛛 🆓 Contig 🔣 Monitor 🛛 🔩 Admin		
Virtual Contexts 👻 Operations			
System	Config >Virtual Contexts >Security >ACLs		li i
Load Balancing	🔹 🗠 🗷 📴 🤋 VC_web 🕑		
53.	ACLS		
Security	Nome*: ACL_permit_al		
- ACLs	Type*:   Extended  EtherType		
<ul> <li>Object Groups</li> </ul>	Remark:		
Network.		Deploy Now Cancel 🛛 🕨	Delete
High Availability (HA)	Extended		
HA Tracking and Failure Detection	Extended @ ACL_permit_all	+ 6 9	7 🖬 🚳
Expert •	Tine No. Permit Service Object Group Protocol Source Network Object Group A		
	1 • 1 • IP (Any)	v	~
<		✓ Configurations are in sync 01-Aux	2008



L

- Step 10 Choose the Access Group tab.
- Step 11 Click Add above the pane (Figure 4-5).

#### Figure 4-5 Adding an ACL to an Interface

ahaha	A	CE 4710 Device M	anager A3(1.0)		Welcome admin	Logout + Hel
cisco		🦓 Config 🛛 ෫	🔄 Monitor 🛛 📑 Admin			
Virtual Contexts 👻 Operat	tions					
System	I summaries		exts >Network >VLAN Interf	aces		_
Load Balancing	, 1919	C.ne	b 🔽			
551.	VLAN	Interfaces			🔹 🗹 🗷 I	7 🖻 🖗 🔂
Security	+	🕅 VLAN 🐃	Description	IP Address	Netmask.	Admin Status
Network	- 1 (		nt sice VLAN interface	10.10.40.1	255.255.255.0	Up
- Port Channel Interfaces	2 (	500 Serr	rver side VLAN interface	10.10.50.1	255.255.255.0	Up
<ul> <li>GgabitEthernet Interfaces</li> </ul>						
<ul> <li>VLAN Interfaces</li> </ul>						
<ul> <li>BVI Interfaces</li> </ul>						
- Static Routes						
<ul> <li>Global IP DHCP</li> </ul>						
High Availability (HA)	•					
HA Tracking and Failure Detection	•					
HA Tracking and Failure Detection Expert	-					
	-					
	Policy	Access Group Static	ARP Entries NAT Pool DHCP Relay C	onliguration		
	Policy Acces	is Group @ 400	ARP Extrins NAT Pool DHCP Relay C	configuration		
	Policy Acces			ionfiguration		
	Policy Acces	is Group @ 400	ermit_all	ionfiguration )		
	Policy Acces	is Group @ 400 CL Name <sup>®</sup> : ③ ACL_pe	ermit_all	onfiguration	Deploy Now C	Cancel
	Policy Acces	is Group @ 400 CL Name <sup>®</sup> : ③ ACL_pe	ermit_all	ionAgaration	Deploy Now C	Cancel
	Policy Acces	is Group @ 400 CL Name <sup>®</sup> : ③ ACL_pe	ermit_all	ionfiguration	Deploy Now C	Cancel
	Policy Acces	is Group @ 400 CL Name <sup>®</sup> : ③ ACL_pe	ermit_all	ionfiguration	Deploy Now C	Cancel 🔀
	Policy Acces	is Group @ 400 CL Name <sup>®</sup> : ③ ACL_pe	ermit_all	ionflywration ]	Deploy Now C	Cancel 🔀
	Policy Acces	is Group @ 400 CL Name <sup>®</sup> : ③ ACL_pe	ermit_all	ionfiguration ]	Deploy Now C	Cancel
	Policy Acces	is Group @ 400 CL Name <sup>®</sup> : ③ ACL_pe	ermit_all	ionfiguration ]	Deploy Now C	Cancel
	Policy Acces B TA TOrec	is Group @ 400 CL Name <sup>®</sup> : ③ ACL_pe	ermit_all	ionfiguration ]	Deploy Now C	Cancel
	Policy Acces	is Group @ 400 CL Name <sup>®</sup> : ③ ACL_pe	ermit_all	infiguration ]	Deploy Now C	Cancel

**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 4-6).

### Figure 4-6 ACL is Added to an Interface

ahaha	ACE 4/10 D	evice Manager A3(1.0)		Welcome admin	Logout • He
CISCO	🔹 🗞 Carli	a 🛛 💐 Monitor 🛛 📑 Admin			
Virtual Contexts   Operation	15				
System		al Contexts >Network >VLAN Into	erfaces		_
Load Balancing		? VC_web 💌			
59.	VLAN Interfaces			🔹 🗹 🕱 I	7 🖻 🖗 🚮
Security	► VLAN	Description	IP Address	Netmask.	Admin Status
Network	<b>v</b> 1 💿	400 Client sice VLAN interface	10.10.40.1	255.255.255.0	Up
Port Channel Interfaces	2 ()	500 Serrver side VLAN interface	10.10.50.1	255.255.255.0	Up
GgabitEthernet Interfaces					
VLAN Interfaces					
BVI Interfaces					
Static Routes					
Global IP DHCP					
annear er er rer					
High Availability (HA)	•				
High Availability (HA)	•				
High Availability (HA) HA Tracking and Fallure Detection					
High Availability (HA)	6 6				
High Availability (HA) HA Tracking and Fallure Detection					
High Availability (HA) HA Tracking and Fallure Detection	Policy Access fire		ay Configuration		
High Availability (HA) HA Tracking and Fallure Detection	Poky Access Group @	400	ay Configuration		* 9 7 6
High Availability (HA) HA Tracking and Fallure Detection	Access Group @	400 ● \$ACL Name	ay Configuration	Direction	• 3 7 4
High Availability (HA) HA Tracking and Falure Detection	1	400	ay Configuration		• 3 🗸
High Availability (HA) HA Tracking and Failure Detection	Access Group @	400 ● \$ACL Name	ay Configuration	Direction	• • •
High Availability (HA) HA Tracking and Failure Detection	Access Group @	400 ● \$ACL Name	ay Configuration	Direction	+ <u>9</u> 7 H
High Availability (HA) HA Tracking and Failure Detection	Access Group @	400 ● \$ACL Name	ay Configuration	Direction	* 3 7 4
High Availability (HA) HA Tracking and Fallure Detection	Access Group @	400 ● \$ACL Name	ay Configuration	Direction	• 9 🖓 🖬
High Availability (HA) HA Tracking and Fallure Detection	Access Group @	400 ● \$ACL Name	ay Configuration	Direction	
High Availability (HA) HA Tracking and Fallure Detection	Access Group @	400 ● \$ACL Name	ay Configuration	Direction	* 3 7 6
High Availability (HA) HA Tracking and Fallure Detection	Access Group @	400 ● \$ACL Name	ay Configuration	Direction	* 3 7 6.
High Availability (HA) HA Tracking and Falure Detection Expert	Access Group #	400 ● \$ACL Name	ay Configuration	Direction	* 3 7 -
High Availability (HA) HA Tracking and Falure Detection	Access Group @	400 ● \$ACL Name		Direction	

# Configuring an ACL Using the CLI

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

Step 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#

**Step 2** Enter configuration mode.

host1/VC\_web# Config host1/VC\_web(config)#

Step 3 Create an ACL.

host1/VC\_web(config)# access-list INBOUND extended permit ip any any

**Step 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

Step 5 Display the ACL configuration information.

host1/VC\_web(config)# exit
host1/VC\_web# show running-config access-list

In this chapter, 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.

#### Cisco 4700 Series Application Control Engine Appliance Quick Start Guide



CHAPTER 5

# Configuring Role-Based Access Control

This chapter describes how to configure role-based access control (RBAC) on the Cisco 4700 Series Application Control Engine (ACE) appliance. This chapter contains the following sections:

- Overview
- Configuring RBAC Using the Device Manager GUI
- Configuring RBAC Using the CLI

## **Overview**

After reading this chapter, you should have a basic understanding of how the ACE appliance provides security administration by using RBAC and how to configure a server maintenance user with permission to access a subset of your network.

One of the most challenging problems in managing large networks is the complexity of security administration. The ACE appliance allows you to determine the commands and resources available to each user through RBAC. In RBAC, users are associated with domains and roles.

A domain is a collection of physical and virtual network resources such as real servers and virtual servers.

User roles determine a user's privileges, such as the commands that the user can enter and the actions the user can perform in a particular context. The ACE provides a number of predefined roles. In addition, administrators in any context can define new roles.

The ACE provides the following predefined roles, which you cannot delete or modify:

- Admin—If created in the Admin context, has complete access to, and control over, all contexts, domains, roles, users, resources, and objects in the entire ACE. If created in a user context, gives a user complete access to and control over all policies, roles, domains, server farms, real servers, and other objects in that context.
- Network Admin—Has complete access to and control over the following features:
  - Interfaces
  - Routing
  - Connection parameters
  - Network Address Translation (NAT)
  - VIPs
  - Copy configurations
  - changeto command
- Network-Monitor—Has access to all **show** commands and to the **changeto** command. If you do not explicitly assign a role to a user with the **username** command, this is the default role.
- Security-Admin—Has complete access to and control over the following security-related features within a context:
  - ACLs
  - Application inspection
  - Connection parameters
  - Interfaces
  - Authentication, authorization, and accounting (AAA)
  - NAT

- Copy configurations
- changeto command
- Server-Appln-Maintenance—Has complete access to and control over the following features:
  - Real servers
  - Server farms
  - Load balancing
  - Copy configurations
  - changeto command
- Server-Maintenance—Can perform real server maintenance, monitoring, and debugging for the following features:
  - Real servers-Modify permission
  - Server farms—Debug permission
  - VIPs—Debug permission
  - Probes—Debug permission
  - Load balancing—Debug permission
  - changeto command—Create permission
- SLB-Admin—Has complete access to and control over the following ACE features within a context:
  - Real servers
  - Server farms
  - VIPs
  - Probes
  - Load balancing (Layer 3/4 and Layer 7)
  - NAT
  - Interfaces
  - Copy configurations
  - changeto command

- SSL-Admin—Can administer all SSL features:
  - SSL—Create permission
  - PKI—Create permission
  - Interfaces—Modify permission
  - Copy configurations—Create permission
  - changeto command—Create permission

You can create a user and assign them privileges through RBAC as follows:

- Step 1 Create a domain and choose network resources for the domain.
- **Step 2** Create a user and associate the user with the following:
  - A role (predefined or custom)
  - A domain

This chapter describes how to create a domain and a user, and how to associate the user with a predefined role and the new domain. For more information on predefined roles and how to define a custom role, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide.* 

To create a domain and a user, you can use either the ACE Device Manager GUI or the CLI.

# **Configuring RBAC Using the Device Manager GUI**

In this procedure, you use the GUI to create a domain that includes the user context that you created in Chapter 3, "Creating a Virtual Context," and then create a server maintenance user, user1, to manage those servers. Configure this RBAC setup using the GUI by following these steps:

- Step 1 Choose VC\_web.
- Step 2 Choose Admin > Role-Based Access Control > Domains. The Domains pane appears (Figure 5-1).

### Figure 5-1 Domains Pane

cisco	ACE 4719 Device Manager A3(1.9)	Welcome admin Logout + Hel
	Device Management   Tools	
Users	Admin > Role-Based Access Control > Domains	
Active Users	🔷 🔍 🔿 🗶 Wmb 🔍	
Roles	Domains	🗠 🖬 🖸 🖬 🔂
Domains	Comain Name	All Objects
Conde G	I 💿 derfault-domain	~
6	3	

Step 3 Click Add to add a new domain. The New Domain window appears (Figure 5-2).

cisco	ACE 4718 Device Manager A3(1.8)	Welcome admin	Logout • Help
	Device Management - Tools		
Users	Admin > Role-Based Access Control > Domains		0
Active Users	Domains		
Roles	Domain Name*: Domain1		
Domains	All Objects:		
		Deploy Now C	ancel 🔀
<u>(</u>	>		LP81.20
Ready		Configurations are in sync 044	kup-2008

#### Figure 5-2 Domains Window

- Step 4 Enter **Domain1** for the Domain Name.
- Step 5 Select All Objects.
- Step 6 Click Deploy Now to create a domain that includes all objects in context VC\_web.
- Step 7 Choose Role-Based Access Control > Users to create a user. The Users pane appears (Figure 5-3).

#### Figure 5-3 Users Pane

ahaha	~	CE 4710 Device Manager A3	(1.0)	Welco	me admin Logout • He
CISCO		🦓 Config 🛛 🔌 Monitor	🥦 Admin		
Role-Based Access Control	Device Management				
Isers		Role-Based Access Control	Users		
Active Users		💽 2. VC.,web ⊻			
toles	Users				💌 🛛 🖬 🖗
Comains		Cliser Name	Expiry Date No records	■ Role	■ Domains

Step 8 Click Add. The User window appears (Figure 5-4).

#### Figure 5-4 Users Window

cisco	ACE 4718 Device Manager A2(1.8)	Welcome admin	Logout • Help
Role-Based Access Control			
Users	Admin>Role-Based Access Control>Users		<sup>1</sup>
Active Users	Users		
Roles	Ubers SUber Name* : user1		
Domains	Expiry Date:		
	Password Entered As*: @ Clear Text O Encrypted Text		
	Password*: Confirm:		
	■Role* : Server-Maintenance		
	Comains* : Available Items Selected Items		
	default-domain		
		Deploy Now C.	iancel
			3
<	>		Aug-2008
Ready		Configurations are in sync 044	4ug-2008

- Step 9 Enter the following user attributes. Leave the remaining attributes blank or with the default values.
  - User Name: user1
  - Password: MYPASSWORD
  - Confirm: MYPASSWORD
  - Role: Server-Maintenance
- Step 10 Choose Domain1 and click the right-arrow button. Domain1 is moved to the Selected Items list.
- Step 11 Choose default-domain and click the left-arrow button. Default-domain is removed from the Selected Items list.

Step 12 Associate the new user user1 with the role Server-Maintenance and the domain Domain1 by clicking Deploy Now. The new user is added to the Users pane (Figure 5-5).

#### Figure 5-5 Users Pane with user1 Added

cisco		E 4710 Device Mana; 🍓 Config 🛛 💐 M			Welcome admin Logout + Hel
Role-Based Access Control	. Design Management				
Role-Based Access Control		<ul> <li>Tools</li> <li>Ie-Based Access Co</li> </ul>	antrol Users		
Users			<u>v</u>		
Active Users Roles	Users		_		• • • • • •
Domains		Cuser Name	Expiry Date	∎Role	Domains
	1 💿 user1			Server-Maintenance	Domain1
¢	3				

# **Configuring RBAC Using the CLI**

Configure RBAC using the CLI by following these steps:

Step 1 Verify that you are operating in the desired context by checking the CLI prompt. If necessary, change to the correct context.

host1/Admin# changeto VC\_web
host1/VC\_web#

**Step 2** Enter configuration mode.

host1/VC\_web# Config host1/VC\_web(config)#

**Step 3** Create a domain for the context.

host1/VC\_web(config)# domain Domain1 host1/VC\_web(config-domain)#

Step 4 Allocate all objects in the VC\_web context to the domain.

host1/VC\_web(config-domain)# add-object all host1/VC\_web(config-domain)# exit host1/VC\_web(config)#

Step 5 Configure new user user1, and assign the predefined role TECHNICIAN and the domain Domain1 to the user.

host1/VC\_web(config)# username user1 password 5 MYPASSWORD role TECHNICIAN domain Domain1

**Note** The parameter 5 for password is for an MD5-hashed strong encryption password. Use 0 for a clear text password.

host1/VC\_web(config)# exit

**Step 6** Display the user and domain configurations.

host1/VC\_web# show running-config role host1/VC\_web# show running-config domain

In this chapter, you have created a user to perform a limited number of functions on a subset of your network. Next, you will create a virtual server for server load balancing.

#### Cisco 4700 Series Application Control Engine Appliance Quick Start Guide



CHAPTER 6

# **Configuring Server Load Balancing**

This chapter describes how to configure server load balancing on the Cisco 4700 Series Application Control Engine (ACE) appliance. This chapter contains the following sections:

- Overview
- Configuring Layer 7 Server Load Balancing Using the Device Manager GUI
- Configuring Layer 7 Server Load Balancing Using the CLI

## **Overview**

After reading this chapter, you should have an understanding of the basic server load-balancing capabilities provided by the ACE appliance. You should also be able to configure a virtual server for Layer 7 load-balancing purposes.

When there is a client request for web services, a load-balancing device decides to which server it should send the request. For example, a client request may consist of an HTTP GET for a web page or an FTP GET to download a file. The ACE, as a server load balancer, selects a server that can successfully fulfill the client request in the shortest amount of time without overloading either the server or the server farm as a whole.

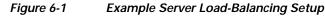
The ACE uses a virtual server to intercept web traffic to a website. A virtual server allows multiple real servers to appear as one for load-balancing purposes. A virtual server, also called a Virtual IP (VIP), is defined by its IP address, the protocol used (for example, UDP or TEC), and the port address.

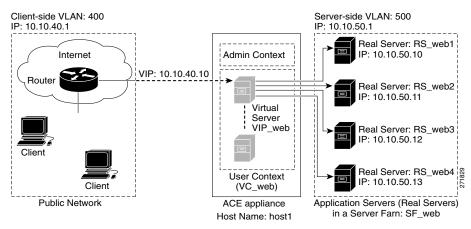
Multiple servers grouped together in server farms are assigned to each virtual server and the ACE appliance carries out load balancing across them. Real servers are dedicated servers that provide services to clients—for example, delivery of HTTP or XML content. Server farms contain the same content and typically reside in the same physical location in a data center.

You can configure the ACE for server load balancing by following these steps:

- **Step 1** Create a virtual server.
- Step 2 Configure the real servers and associate them with a server farm.
- Step 3 Assign the server farm to the virtual server.
- Step 4 Deploy the configuration.

This chapter describes how to configure a virtual server using either the Device Manager GUI or the CLI, using the network setup example illustrated in Figure 6-1.





The configuration of the example setup is as follows:

- A virtual server VS\_web is created with a virtual IP address 10.10.40.10 to forward the client traffic from VLAN 400 to the application servers in VLAN 500.
- There are four real servers grouped into the server farm SF\_web.
- The virtual server uses a round-robin predictor to forward the client requests to one of the real servers in the server farm.

# Configuring Layer 7 Server Load Balancing Using the Device Manager GUI

You can configure Layer 7 server load balancing using the Device Manager GUI by following these steps:

Step 1 Choose Load Balancing > Virtual Servers. The Virtual Servers pane appears (Figure 6-2). Choose the user context VC\_web.

#### Figure 6-2 Virtual Servers Pane

de de	ACE 4710 Devi	ce Manager A3(	1.0}			Welcome adm	in Logout • Help
cisco	🚱 Conha	Monitor	in Admin				
Virtual Contexts 👻 Operations							
System 🕨	Config > Virtual C		Balancing > Virt	ual Ser	vers		Υ.
Load Balancing 🔹		VC_web 💌					
Virtual Servers	Virtual Servers						+ 61 Y H-
- Real Servers	Name	Configured State	VIP Address	Port	VLANS	Server Farms	Virtual Context
- Server Farms	That is	Contrigation Scale		records	TENTE	Server	
Health Monitoring							
Stickiness							
Parameter Maps							
Secure KAL-AP							
59. <b>•</b>							
Security •							
Network.							
High Availability (HA)							
HA Tracking and Failure Detection							
Expert +							
>							
Ready						onfigurations are in sync	

Step 2 Click Add to add a new virtual server. The Virtual Server configuration window appears (Figure 6-3).

	ACE 4719 Device Manager A3(1.9) Welcom	e admin Logout • Help
ahaha		e source expressioner
CISCO	🗧 🦓 Config 🔣 Monitor 🛛 🔩 Admin	
Virtual Contexts + Operations		
System	Config > Virtual Contexts > Load Balancing > Virtual Servers > Add	0
Load Balancing	🔹 🗟 📀 💽 🙁 VC_meb 🔍	
- Virtual Servers	Creating Virtual Server on Virtual Context VC_web	
- Real Servers		
- Server Farms	*Properties	
<ul> <li>Health Monitoring</li> </ul>	V3P Name* : V3P_web	
- Stickiness	V3P 3P* : 10.10.40.10	
> Parameter Maps		
- Secure KAL-AP	Call Out Coop	
	Application Protocol": http 🔽	
Security	<ul> <li>Port*: 80</li> </ul>	
Network P	Al VLANS:	
High Availability (HA)	VLAN* : Available Items Selected Items	
HA Tracking and Falure Detection	500 400	
Epert	2	
	Pefault L7 Load-Balancing Action	
	Action*: Action*:	
	Primary Action* : loadbalance 🗸	
	Server Form" :	
	Badiup Serverfam:	
	Enable Compression (Deflate Method):	
		Deploy Now Cancel
< >	8	87
Ready	✓ Configurations a	re in sync 04-Aug-2008

#### Figure 6-3 Properties in the Virtual Server Configuration Window

By default, the Basic View configuration option is selected and the Properties section is open.

- **Step 3** In Properties, enter the following virtual server attributes. Leave the remaining attributes blank or with their default values.
  - VIP Name: VS\_web
  - VIP IP: 10.10.40.10



Note A client request targeted at a website (a URL) is translated to an IP address according to the Domain Name System (DNS). A virtual IP address assigned to a virtual server is the IP address that corresponds to the URL of the website from which the client requests services.

- Protocol: TCP
- Application Protocol: HTTP
- Port: 80
- VLAN: 400
- Step 4 In the Default L7 Load-Balancing Action section, choose loadbalance from the Primary Action drop-down list.
- Step 5 Choose \*New\* from the Server Farm drop-down list to configure a new server farm.
- **Step 6** Enter the following server farm attributes. Leave the remaining attributes blank or with their default values.
  - Name: SF\_web
  - Type: host
  - Predictor: roundrobin
- Step 7 Click Add to add a new entry to the Real Servers pane. A new entry appears in the Real Servers pane (Figure 6-4).

ahaha	ACE 4710 Device Manager A3(1.0)	Welcome admin
CISCO	🖧 Conto 🔣 Monitor 📑 Admin	
Virtual Contexts 👻 Operations		
System	Config >Virtual Contexts >Load Balancing >Virtual Servers >Add	
System		

#### Figure 6-4 Real Servers Pane in the Virtual Server Configuration Window

Virtual Contexts    Operations	_				
System		Virtual Contexts >Load B	alancing >Virtual Ser	vers > Add	<b>D</b>
Load Balancing	و الألف ا	× 💽 9 VC_meb 💌			
- Virtual Servers	•Default	L7 Load-Balancing Action			^
Real Servers     Servers Famis     Health Monitoring     Sockness     Parameter Maps     Sockerss     Socker KAL-AP     SSL     Socker KAL-AP     SSL     Network     High Availability (HA)     High Availability (HA)	Action* :	Primary Action* : Server Farm* :	Ioadbalance v "New" v Name" : Type" : Partial-threshold Percentage: Back Inservice: Fall Action: Transparent:	© © N/A C Purge © N/A C False C True	
Expert			Predictor" : Probes:	Roundrobin V Available Items Selected Items Create	
			Real Servers" :	PName*:       P InS_web1       C InS_web1         IP Address:       10.1.18.2         IP Address:       IP Instance         IP Address:       IP Instance         IP Address:       IP Instance         IP Address:       IP Instance         IP Instance       Out of Service         OX       Cancel	
		Backup Serverfarm: Enable Compression (Deflate Method)			
< >				Deploy Now Cancel	Ť
Ready				✓ Configurations are in sync 01-Aug-2008	

- **Step 8** Enter the following attributes for the first real server to be configured. Leave the remaining attributes blank or with their default values.
  - Name: RS\_web1
  - IP Address: 10.10.50.10
  - Port: 80
  - Weight: 8
  - State: In Service

Click **OK** to save the attributes of the first real server.

Logout . Help



For information on how to configure a health probe, see Chapter 10, "Configuring Health Monitoring Using Health Probes."

**Step 9** Add three more entries to the Real Servers pane by repeating Steps 7 and 8 with the following real server names and corresponding IP addresses. Leave the remaining attributes with their default values.

For RS\_web2, enter:

- Name: RS\_web2
- IP Address: 10.10.50.11
- Port: 80

For RS\_web3, enter:

- Name: RS\_web3
- IP Address: 10.10.50.12
- Port: 80

For RS\_web4, enter:

- Name: RS\_web4
- IP Address: 10.10.50.13
- Port: 80
- **Step 10** Click **Deploy Now** at the bottom of the window to save your settings for the virtual server. The Virtual Servers pane reappears (Figure 6-5). The newly configured virtual server appears in the pane and is in the Inservice state, which means that the virtual server is in use as a destination for server load balancing.

#### Figure 6-5 Virtual Servers Pane with a Virtual Server Created

ahaha	ACE 4710 I	evice Manager A3(1	.+)		Welcome a	dmin Logout • He
CISCO	🛛 🖧 con	lo 🛃 Monitor	Reference Admin			
Virtual Contexts    Operations						
System	Config >Virtual C		cing > Virtual Server:			
Load Balancing -		C]weo 💌				
	rirtual Servers					• 🗹 🧿 🔽 🖬
Real Servers	Name	Configured State	VIP Address	Port VLANS	Server Farms	Virtual Context
Server Fanns	1 💽 VIP_web	V Inservice	10.10.40.10	http:80 400	SF_web	VC_web
Health Monitoring						
Parameter Maps						
Secure KAL-AP						
53.						
Security >						
Network						
High Availability (HA)						
HA Tracking and Failure Detection						
Expert >						

# Configuring Layer 7 Server Load Balancing Using the CLI

You can configure Layer 7 server load balancing using the command-line interface (CLI). This section contains the following topics:

- Configuring Real Servers
- Creating a Server Farm
- Creating a Virtual Server Traffic Policy

### **Configuring Real Servers**

Configure real servers on the ACE using the CLI by following these steps:

Step 1	Verify that you are operating in the desired context by checking the CLI prompt. If necessary, change to the correct context.
	host1/Admin# <b>changeto VC_web</b> host1/VC_web#
Step 2	Enter configuration mode.
	host1/VC_web# config
Step 3	Create a real server named RS_web1 as type host (the default).
	<pre>host1/VC_web(config)# rserver RS_web1 host1/VC_web(config-rserver-host)#</pre>
Step 4	Enter a description of the real server.
	<pre>host1/VC_web(config-rserver-host)# description content server web-one</pre>
Step 5	Assign the real server with an IP address of 10.10.50.10.
	<pre>host1/VC_web(config-rserver-host)# ip address 10.10.50.10</pre>
Step 6	Place the real server in service and exit configuration mode.
	<pre>host1/VC_web(config-rserver-host)# inservice host1/VC_web(config-rserver-host)# exit host1/VC_web(config)#</pre>

**Step 7** Add three more real servers by repeating Steps 3 through 6, using the following real server names, descriptions, and IP addresses.

For RS\_web2, enter:

- Name: RS\_web2
- Description: content server web-two
- IP Address: 10.10.50.11

For RS\_web3, enter:

- Name: RS\_web3
- Description: content server web-three
- IP Address: 10.10.50.12

For RS\_web4, enter:

- Name: RS\_web4
- · Description: content server web-four
- IP Address: 10.10.50.13

**Step 8** Display the configuration of the real servers.

host1/VC\_web(config)# do show running-config rserver

### **Creating a Server Farm**

After you create and configure the real servers, you can create a server farm and associate the real servers with it. Create a server farm by following these steps:

Step 1	Create a server farm of type host (the default) named SF_web.
	host1/VC_web(config)# <b>serverfarm SF_web</b> host1/VC_web(config-sfarm-host)#
Step 2	Associate real server RS_web1 to the server farm through port 80.

**Step 3** Place the real server in service within the server farm and exit configuration mode.

```
host1/VC_web(config-sfarm-host-rs)# inservice
host1/VC_web(config-sfarm-host-rs)# exit
host1/VC_web(config-sfarm-host)#
```



- Before you can start sending connections to a real server in a server farm, you must place it in service. Otherwise, the ACE considers it out of service and the server farm cannot receive or respond to client requests.
- Step 4 Similarly, associate the RS\_web2, RS\_web3, and RS\_web4 real servers with the SF\_web server farm.

```
host1/VC_web(config-sfarm-host)# rserver RS_web2 80
host1/VC_web(config-sfarm-host-rs)# inservice
host1/VC_web(config-sfarm-host-rs)# exit
host1/VC_web(config-sfarm-host)# rserver RS_web3 80
host1/VC_web(config-sfarm-host-rs)# inservice
host1/VC_web(config-sfarm-host-rs)# exit
host1/VC_web(config-sfarm-host-rs)# exit
host1/VC_web(config-sfarm-host-rs)# inservice
host1/VC_web(config-sfarm-host-rs)# inservice
host1/VC_web(config-sfarm-host-rs)# inservice
```

**Step 5** Exit server farm configuration mode.

```
host1/VC_web(config-sfarm-host) # exit
host1/VC_web(config) #
```

**Step 6** Display the information for the real servers and verify that the real servers appear as operational (even though network connectivity has not been established).

```
host1/VC_web(config)# do show rserver RS_web1
host1/VC_web(config)# do show rserver RS_web2
host1/VC_web(config)# do show rserver RS_web3
host1/VC_web(config)# do show rserver RS_web4
```

Step 7 Display how the ACE populates the ARP table with the real servers.

host1/VC\_web(config)# do show arp

### **Creating a Virtual Server Traffic Policy**

You can create a virtual server traffic policy on the ACE by following these steps:

**Step 1** Create a Layer 7 server load-balancing policy map named PM\_LB to match the class maps in the order in which they occur for load balancing.

```
host1/VC_web(config)# policy-map type loadbalance first-match PM_LB
host1/VC_web(config-pmap-lb)#
```



The ACE uses a class map to specify a series of flow match criteria (traffic classifications). The ACE uses a policy map to define a series of actions (functions) that you want applied to a set of classified inbound traffic.

**Step 2** For a simple load-balancing policy, assign the ACE default class map which contains an implicit match any statement to match any traffic classification.

```
host1/VC_web(config-pmap-lb)# class class-default
host1/VC_web(config-pmap-lb-c)#
```

**Step 3** Add the server farm SF\_web to the Layer 7 server load-balancing policy map and exit configuration mode.

```
host1/VC_web(config-pmap-lb-c)# serverfarm SF_web
host1/VC_web(config-pmap-c)# exit
host1/VC_web(config-pmap)# exit
host1/VC_web(config)#
```

Step 4 Create a Layer 3 and Layer 4 load-balancing class map VS\_web.

host1/VC\_web(config)# class-map VS\_web
host1/VC\_web(config-cmap)#

Step 5 Define a match statement for the IP address 10.10.40.10 for any IP protocol and exit configuration mode.

```
host1/VC_web(config-cmap)# match virtual-address 10.10.40.10
255.255.255.0 tcp eq 80
host1/VC_web(config-cmap)# exit
host1/VC_web(config)#
```

**Step 6** Create a Layer 3 and Layer 4 multi-match policy map to direct classified incoming requests to the load-balancing policy map.

```
host1/VC_web(config)# policy-map multi-match PM_multi_match
host1/VC_web(config-pmap)#
```

Step 7 Associate the Layer 3 and Layer 4 class map VS\_web with the policy map.

host1/VC\_web(config-pmap)# class VS\_web host1/VC\_web(config-pmap-c)#

Step 8 Associate the Layer 7 load-balancing policy map PM\_LB with the Layer 3 and Layer 4 policy map.

host1/VC\_web(config-pmap-c)# loadbalance policy PM\_LB host1/VC\_web(config-pmap-lb-c)#

Step 9 Enable a VIP for load-balancing operations and exit configuration mode.

```
host1/VC_web(config-pmap-lb-c)# loadbalance vip inservice
host1/VC_web(config-pmap-c)# exit
host1/VC_web(config-pmap)# exit
host1/VC_web(config)#
```

Step 10 Access the interface to which you want to apply the multi-match policy map.

host1/VC\_web(config)# interface vlan 400
host1/VC\_web(config-if)#

**Step 11** Apply the multi-match policy map PM\_multi\_match.

```
host1/VC_web(config-if)# service-policy input PM_multi_match
host1/VC_web(config-if)# exit
host1/VC_web(config)#
```

**Step 12** Save the running configuration to the startup configuration.

host1/VC\_web(config)# do copy running-config startup-config

**Step 13** Display the service policy state for the PM\_multi\_match policy map.

host1/VC\_web(config)# do show service-policy PM\_multi\_match

In this chapter, you have configured a virtual server for load-balancing HTTP traffic. In the next chapter, you will configure a load-balancing predictor to forward client requests to the appropriate real servers.



CHAPTER 7

# Configuring a Load-Balancing Predictor

This chapter describes how to configure a load-balancing predictor on the Cisco 4700 Series Application Control Engine (ACE) appliance. This chapter contains the following sections:

- Overview
- Configuring a Hash Header Predictor Using the Device Manager GUI
- Configuring a Hash Header Predictor Using the CLI

### **Overview**

After reading this chapter, you should have a basic understanding of how the ACE appliance selects a real server for a client request using a predictor and how to configure a hash header predictor as an example.

When there is a client request for web services, the ACE selects a server that can successfully fulfill the client request in the shortest amount of time without overloading either the individual server or the server farm.

The ACE makes load-balancing choices using a predictor. When you configure a predictor, you define the series of checks and calculations that the ACE will perform to determine which real server can best service a client request.

For each server farm, you can configure one of several predictor types to allow the ACE to select an appropriate server. Two common predictor types include the following:

- Round-robin—Selects a server from the list of real servers based on weighted server capacity. A weight can be assigned to each real server based on its connection capacity in relation to the other servers in a server farm. Servers with higher weight values receive a proportionally higher number of connections than servers with lower weight values. For example, a server with a weight of 5 would receive five connections for every one connection received by a server with a weight of 1. Also known as weighted round-robin, this is the default predictor.
- Hash header—Selects a server using a hash value based on the HTTP header name.

For a complete list of predictor types that the ACE supports and how to configure them, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

You can configure a server load-balancing predictor by following these steps:

Step 1 Choose a server farm.

**Step 2** Choose a predictor type and its parameters.

Step 3 Deploy the configuration.

This chapter describes how to configure a hash header predictor for the server farm that was created in Chapter 6, "Configuring Server Load Balancing," as illustrated in Figure 6-1. You can use either the ACE Device Manager GUI or the CLI.

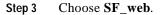
# Configuring a Hash Header Predictor Using the Device Manager GUI

You can configure a hash header predictor using the ACE Device Manager GUI by following these steps:

- Step 1 Choose Config > Virtual Contexts. Choose context VC\_web.
- Step 2 Choose Load Balancing > Server Farms. The Server Farms pane appears (Figure 7-1).

#### Figure 7-1 Configuring a Predictor

ahaha	ACE 4710 Device Manager A3(1.0)		Welcome admin	Logout + Help
CISCO	🦓 Config 🔍 Monitor 📑	Admin		
Virtual Contexts 👻 Operation	6			
System	Config > Virtual Contexts > Load Balancing	Server Farms		8
Load Balancing	🖕 🏟 🖉 🖉 🧟 VC_web 💌			
<ul> <li>Virtual Servers</li> </ul>	Server Farms		🛨 🖬 🗎	7 🖬 🤁 🔂
- Real Servers	Name	Type	Description	
Server Farms     Health Monitoring	1 💽 SF_web	Host		
- Sidness				
> Parameter Maps				
- Secure KAL-AP				
59.	•			
Security	•			
Network	•			
High Availability (HA)	•			
HA Tracking and Falure Detection	•			
Expert	•			
	Real Servers Predictor Ratcode Map			
	Predictor @ SF_web			
	Type*: Hash_Header 💌			
	Header Name* : C Accept	*		
<	3			Deploy Now
Ready			Configurations are in sync 04-4	ug-2008



- Step 4 Choose the **Predictor** tab.
- Step 5 Choose Hash\_Header for the predictor Type.
- Step 6 Choose Accept for the Header Name.
- Step 7 Assign the hash header predictor to server farm SF\_web by clicking **Deploy Now**.

## **Configuring a Hash Header Predictor Using the CLI**

You can configure a hash header predictor using the CLI by following these steps:

Step 1Verify that you are operating in the desired context by checking the CLI prompt.<br/>If necessary, change to the correct context.

host1/Admin# changeto VC\_web
host1/VC\_web#

Step 2 Enter configuration mode for SF\_web.

host1/VC\_web# config host1/VC\_web(config)# serverfarm SF\_web host1/VC\_web(config-sfarm-host)#

Step 3 Configure a hash header predictor.

host1/VC\_web(config-sfarm-host)# predictor hash header Accept

Step 4 Display the predictor configuration information.

host1/VC\_web(config-sfarm-host)# exit host1/VC\_web(config)# exit host1/VC\_web# show running-config serverfarm

In this chapter, you have configured a hash header predictor for your server load balancing. Next, you will configure server persistence by using the stickiness feature.



CHAPTER **8** 

# **Configuring Server Persistence Using** Stickiness

This chapter describes how to configure server persistence using stickiness on the Cisco 4700 Series Application Control Engine (ACE) appliance. This chapter contains the following sections:

- Overview
- Configuring HTTP Cookie Stickiness Using the Device Manager GUI
- Configuring HTTP Cookie Stickiness Using the CLI

### **Overview**

After reading this chapter, you should have a basic understanding of how the ACE appliance provides server persistence using stickiness, and how to configure HTTP cookie stickiness.

When customers visit an e-commerce site, they usually start by browsing the site. Depending on the application, the site may require that the client become persisted (stuck) to one server as soon as the initial connection is established, or the application may require this action only when the client starts to create a transaction, such as when building a shopping cart. For example, after the client adds items to a shopping cart, it is important that all subsequent client requests are directed to the same real server so that all the items are contained in one shopping cart on one server. An instance of a customer's shopping cart is typically local to a particular server rather than duplicated across multiple servers.

E-commerce applications are not the only types of applications that require a sequence of client requests to be directed to the same real server. Any web applications that maintain client information may require stickiness, such as banking and online trading applications, or FTP and HTTP file transfers.

The ACE can be configured so that the same client can maintain multiple, simultaneous, or subsequent TCP or IP connections with the same real server for the duration of a session. This session persistence capability of the ACE is called stickiness. A session is defined as a series of transactions between a client and a server over some finite period of time (from several minutes to several hours).

Depending on the configured server load-balancing policy, the ACE sticks a client to an appropriate server after the ACE determines which load-balancing method to use. If the ACE determines that a client is already stuck to a particular server, then the ACE sends that client request to that server, regardless of the load-balancing criteria. If the ACE determines that the client is not stuck to a particular server, it applies the normal load-balancing rules to the request.

To determine how a particular client is stuck to a specific web server and how an application distinguishes each client or a group of clients, the ACE supports the following sticky methods:

- Source and/or destination IP address—For stickiness, you can use the source IP address, the destination IP address, or both to uniquely identify individual clients and their requests based on their IP net masks. However, if an enterprise or service provider uses a mega-proxy (a free, anonymous web proxy service) to establish client connections to the Internet, the source IP address is not a reliable indicator of the true source of the request. In this case, you can use another sticky method to ensure session persistence.
- Cookie—Client cookies uniquely identify clients to the ACE and to the servers that provide content. A cookie is a small data structure within the HTTP header that a server uses to deliver data to a web client, with the request that the client store the information. This information might include items that users have added to their shopping carts or travel dates that they have chosen. When the ACE examines a request for content and determines that the

content is sticky, it examines any cookie or URL present in the content request. The ACE uses the information in the cookie or URL to direct the content request to the appropriate server.

• Hypertext Transfer Protocol (HTTP) header—You can specify a header offset to provide stickiness based on a unique portion of the HTTP header.

The e-commerce application often dictates which of these methods is appropriate for a particular e-commerce application.

The ACE uses sticky groups for stickiness attributes. These attributes include the sticky method, timeout, replication, and attributes related to a particular sticky method.

To track sticky connections, the ACE uses a sticky table with information about sticky groups, sticky methods, sticky connections, and real servers. The ACE uses a configurable timeout mechanism to age out sticky table entries. When an entry times out, it becomes eligible for reuse. High connection rates may cause the premature aging out of sticky entries. In this case, the ACE reuses the entries that are closest to expiration first.

Entries in the sticky table can be either dynamic (generated by the ACE as needed) or static (configured). When you create a static sticky entry, the ACE places the entry in the sticky table immediately, and it remains in the sticky database until you remove it from the configuration.

You can configure stickiness by following these steps:

- Step 1 Ensure that resources are allocated for stickiness.
- Step 2 Create a sticky group.
- **Step 3** Associate the sticky group with a Layer 7 server load-balancing action of a virtual server.
- Step 4 Deploy the configuration.

Figure 8-1 illustrates that in a server load-balancing environment, requests from a client are stuck to real server RS\_web4 in a session.

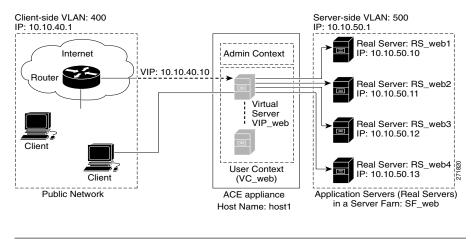


Figure 8-1 Client Requests Stuck to a Server

This chapter describes how to configure stickiness using the HTTP cookie sticky method. For information on how to configure stickiness using the IP address and HTTP header methods, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

# Configuring HTTP Cookie Stickiness Using the Device Manager GUI

You can configure HTTP cookie stickiness using the GUI by following these steps:

- Step 1 Make sure that the context in which you are configuring the sticky group is associated with a resource class that allocates resources to stickiness. See the "Creating a Resource Class" section in Chapter 3.
- Step 2 Choose Load Balancing > Stickiness. The Stickiness pane appears (Figure 8-2).

#### Figure 8-2 Stickiness Pane

	ACE 4710 Devi	ce Manager A3	(1.0)		Welcome admin	Logout + Help
cisco	😽 Conto	Monitor	Admin			
Wrtual Contexts    Operations		7				
	Config > Virtual Conte	xts>Load Bal	ancing > Stickine	55		0
System	🌢 🖉 🕗 🤊 V. met	b 💌				
Load Balancing						
	itickiness					7 <b>- 0</b> 🔂
Real Servers     Server Farms	) Gro	xip Name	Type	Header Name	Cookie N	ame
Health Monitoring				No records		
Stickiness						
Parameter Maps						
Secure KAL-AP						
59.						
Security +						
Network.						
High Availability (HA)						
HA Tracking and Failure Detection						
Expert +						
>						
Ready						

- Step 3 Choose the VC\_web context.
- Step 4 Add a new sticky group by clicking Add. The Stickiness configuration window appears (Figure 8-3).

#### Figure 8-3 Stickiness Configuration Window

cisco	ACE 4710 D	evice Manager A3(1	1.0)	Welcome admin	Logout • Help
Virtual Contexts - Operations			<u> </u>		
System		ntexts >Load Balar	ncing > Stickiness		6
Load Balancing		_web 💌			
- Virtual Servers	- Stickiness				
- Real Servers	Group Name* :	StidyGroup1			
- Server Farms	Type*:	Http_cookie 💌			
<ul> <li>Health Monitoring</li> </ul>	Cookie name* :	Cookie1			
- Stickiness	Enable Insert:				
> Parameter Maps	Offset:				
- Secure KAL-AP		0			
59.	Length:				
Security	Secondary Name:				
Network	Sticky Server Farm:	O ∧/4 ⊙ SF_web			
High Availability (HA)	Backup Server Farm:	⊙ ∧//4 OSF_web			
HA Tracking and Failure Detection	Replicate:				
Expert					
	Timeout:	1440			
	Timeout Active Connections:				
				Deploy Now C	ancel 💽
< >					51.0
Ready				Configurations are in sync 044	
All Conserver				· company of the light	

- **Step 5** Enter the following attributes for the new sticky group. Leave the remaining attributes blank or with their default values.
  - Group Name: StickyGroup1
  - Type: Http\_cookie
  - Cookie name: Cookie1
  - Sticky Server Farm: SF\_web
- Step 6 Add the new sticky group to the Stickiness pane by clicking Deploy Now.

# **Configuring HTTP Cookie Stickiness Using the CLI**

You can configure HTTP cookie stickiness using the CLI by following these steps:

Step 1 Verify that you are operating in the desired context by checking the CLI prompt. If necessary, change to the correct context.

host1/Admin# changeto VC\_web
host1/VC\_web#

**Step 2** Enter configuration mode.

host1/VC\_web# config host1/VC\_web(config)#

Step 3 Create an HTTP-cookie-type sticky group and enter the cookie configuration mode.

```
host1/VC_web(config)# sticky http-cookie Cookiel StickyGroup1
host1/VC_web(config-sticky-cookie)#
```

**Step 4** Configure a timeout for HTTP cookie stickiness.

host1/VC\_web(config-sticky-cookie)# timeout 1440

**Step 5** Associate a server farm with the sticky group and exit configuration mode.

host1/VC\_web(config-sticky-cookie)# serverfarm SF\_web
host1/VC\_web(config-sticky-cookie)# exit
host1/VC\_web(config)# exit
host1/VC\_web#

Step 6 Display the HTTP cookie configuration.

host1/VC\_web# show running-config sticky

In this chapter, you have configured a sticky group using the HTTP-cookie method. In the next chapter, you will configure SSL security.

Configuring HTTP Cookie Stickiness Using the CLI



# CHAPTER 9

# **Configuring SSL Security**

This chapter describes how to configure SSL on the Cisco 4700 Series Application Control Engine (ACE) appliance. This chapter contains the following sections:

- Overview
- Configuring SSL Termination
- Configuring the ACE for SSL Termination Using the Device Manager GUI
- Configuring the ACE for SSL Termination Using the CLI

### **Overview**

After reading this chapter, you should have a basic understanding of how the ACE appliance provides SSL security for your network and how to configure SSL termination, in which the ACE operates as an SSL server.

SSL configuration in an ACE establishes and maintains a SSL session between the ACE and another device. It provides for secure data transactions between a client and a server. SSL provides authentication, encryption, and data integrity in a Public Key Infrastructure (PKI), a set of policies and procedures that establishes a secure information exchange between devices.

In SSL, data is encrypted using one or more symmetric keys that are known only by the two endpoints in the transaction. In a key exchange, one device generates the symmetric key and then encrypts it using an asymmetric encryption scheme before transmitting the key to the other device. Asymmetric encryption requires each device to have a unique key pair consisting of a public key and a private key. A private key is an encryption/decryption key known only to the parties exchanging the messages. A public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures. The two keys are mathematically related; data that is encrypted using the public key can only be decrypted using the corresponding private key, and vice versa.

SSL facilitates client and server authentication through the use of digital certificates. Digital certificates are a form of digital identification to prove the identity of the server to the client, or optionally, the client to the server. A certificate ensures that the identification information is correct and the public key embedded in it actually belongs to the client or server.

A Certificate Authority (CA) issues digital certificates in the context of a PKI. CAs are trusted authorities that sign certificates to verify their authenticity. As the certificate issuer, the CA uses its private key to sign the certificate. Upon receiving a certificate, a client uses the issuer's public key to decrypt and verify the certificate signature to ensure that the certificate was actually issued and signed by an authorized entity.

If you do not have a certificate and the corresponding key pair, you can use the ACE to generate a key pair and a certificate signing request (CSR) to apply for a certificate from a CA. The CA signs the CSR and returns the authorized digital certificate to you. The ACE supports import, export, and other management functions to manage the various certificates and key pair files within each context.

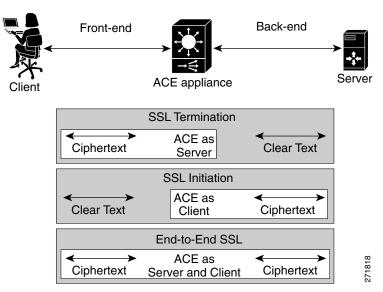
The client and server use the SSL handshake protocol to establish an SSL session between the two devices. During the handshake, the client and server negotiate the SSL parameters that they will use during the secure session. During the SSL handshake, the ACE uses an SSL proxy service, which includes the configuration of SSL session parameters, an RSA key pair, and a matching certificate.

The ACE applies SSL session parameters to an SSL proxy service. Creating an SSL parameter map allows you to apply the same SSL session parameters to different proxy services. The SSL session parameters include timeouts, close protocol behavior, and SSL version—SSL 3 and/or Transport Layer Security (TLS) 1. For more information on these parameters, see the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*.

You can configure the ACE to act as a client or a server during an SSL session by defining operational attributes such as SSL session parameters, SSL key pairs and certificates, and traffic characteristics. When the traffic characteristics match the

settings specified in the operational attributes, the ACE executes the actions associated with the SSL proxy service. Figure 9-1 shows the three basic SSL configurations in which the ACE is used to encrypt and decrypt data between the client and the server: SSL termination, SSL initiation, and end-to-end SSL.





In SSL termination, an ACE context is configured for a front-end application in which the ACE operates as an SSL server that communicates with a client. When you define the flow between an ACE and a client, the ACE operates as a virtual SSL server by adding security services between a web browser (the client) and the HTTP connection (the server).

All inbound SSL flows that come from a client terminate at the ACE. After the connection is terminated, the ACE decrypts the ciphertext (encrypted content) from the client and sends the data as clear text (unencrypted content) to an HTTP server. For information about configuring the ACE for SSL termination, see the "Configuring SSL Termination" section.

In SSL initiation, an ACE context is configured for a back-end application in which the ACE operates as a client that communicates with an SSL server. When you define the flow between an ACE and an SSL server, the ACE operates as a

client and initiates the SSL session. SSL initiation enables the ACE to receive clear text from a client and then establish an SSL session with an SSL server, joining the client and SSL server connections.

The ACE encrypts the clear text that it receives from the client and sends the data as ciphertext to an SSL server. The SSL server can either be an ACE configured for SSL termination (a virtual SSL server) or a real SSL server (web server). On the outbound flow from the SSL server, the ACE decrypts the ciphertext from the server and sends clear text back to the client. For more information on configuring the ACE for SSL initiation, see the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*.

In end-to-end SSL, an ACE context is configured for both SSL termination and SSL initiation. You configure the ACE for end-to-end SSL when you have an application that requires secure SSL channels between the client and the ACE, and between the ACE and the SSL server.

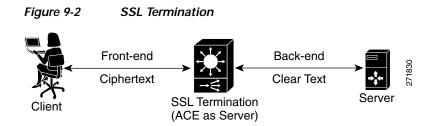
For example, a transaction between banks requires end-to-end SSL to protect all financial information exchanged. End-to-end SSL also allows the ACE to insert load-balancing and security information into the data. The ACE decrypts the ciphertext that it receives and inserts load-balancing and firewall information into the clear text. The ACE then re-encrypts the data and passes the ciphertext to its intended destination. For more information on configuring the ACE for end-to-end SSL initiation, see the *Cisco 4700 Application Control Engine Series Appliance SSL Configuration Guide*.

## **Configuring SSL Termination**

SSL termination occurs when the ACE, acting as an SSL proxy server, terminates an SSL connection from a client and then establishes a TCP connection to an HTTP server. When the ACE terminates the SSL connection, it decrypts the ciphertext from the client and transmits the data as clear text to the HTTP server.

Figure 9-2 shows the following network connections in which the ACE terminates the SSL connection with the client:

- Client to ACE—An SSL connection exists between the client and the ACE acting as an SSL proxy server.
- ACE to Server—A TCP connection exists between the ACE and the HTTP server.



Before configuring the ACE for an SSL operation, you must first configure it for server load balancing. To configure your ACE for server load balancing, see Chapter 6, "Configuring Server Load Balancing."

SSL termination is a Layer 3 and Layer 4 application because it is based on the destination IP address of the inbound traffic flow from the client. When configuring a policy map for SSL termination, you associate the following elements:

- The SSL proxy service, including SSL session parameters, certificate, and key pair.
- The virtual SSL server IP address that the destination IP address of the inbound traffic must match (a class map). When a match occurs, the ACE negotiates with the client to establish an SSL connection.

You can configure the ACE for SSL termination by following these steps:

Import a key file with a key pair.
Import a certificate that matches the imported key pair.
Configure a parameter map.
Configure an SSL proxy service using the key pair, certificate, and parameter map.
Create a virtual server for SSL termination using the SSL proxy service.
Deploy the configuration.

This chapter describes how to configure the ACE for SSL termination using either the Device Manager GUI or the CLI.

# Configuring the ACE for SSL Termination Using the Device Manager GUI

You can configure the ACE for SSL termination using the Device Manager GUI by following these steps:

#### Figure 9-3 Keys Pane

. I I.	ACE 4710 Devic	e Manager A3	(1.0)		Welcome admin	Logout - Help
cisco	🖌 🖓 Conha	Monitor	Nation 🗟			
Virtual Contexts - Operations						
System	Config > Virtual Conte					6
Load Balancing	🔶 🖉 🖉 🖉 🖉 🖓 🖓	×				
eres country .	Keys					🔹 i 🔽 🔤
- Certificates	2Name		Size		Second Law	
- Keys	Visame		SADO	Type No records	Exportable Key	
- Parameter Map				NO FELENDE		
- Chain Group Parameters						
- CSR Parameters						
- Proxy Service						
<ul> <li>Auth Group Parameters</li> </ul>						
<ul> <li>Certificate Revocation List</li> </ul>						
Security +						
Network •						
High Availability (HA)						
HA Tracking and Falure Detection						
Expert						
					Dept Inport Q	rente CR
< >	L				The former of the second secon	
Session will timeout within the next 20 se	econds.				Configurations are in sync 0	HAug-2008

Step 1 Choose the user context VC\_web, and then choose SSL > Keys. The Keys pane appears (Figure 9-3).

**Step 2** Click **Import...** to import a key file. The Import a Certificate/Key File to a Device window appears (Figure 9-4).

Figure 9-4	Import a Certificate/Key File to a Device Window

– Import a Certificate/Key file	to a Device						
Protocol* :	FTP	1					
IP Address* :	172.25.91.10	10					
Remote Filename* :	C:\marketing.	pem					
Local Filename* :	C:\marketing.	pem					
Username* :	admin						
Password* :	•••••		Confirm:	•••••			
Passphrase:			Confirm:				
Nonexportable:							
					ОК	Cancel	

Enter the following parameters. Leave the remaining parameters blank or with their default values.

- Protocol: FTP
- IP Address: 172.25.91.100 (in order for this to work, you should use an IP address where you can access the remote key file)
- Remote Filename: C:\marketing.pem
- Local Filename: C:\marketing.pem
- Username: Admin
- Password: (password for your FTP server)
- Confirm: (retype the password for your FTP server)
- Step 3 Click **OK** to import the key file.
- Step 4 Choose SSL > Certificates. The Certificates pane appears (Figure 9-5).

#### Figure 9-5 Certificates Pane

de de	ACE 4710 Dev	ice Manager A3	(1.0)		Welcome adm	in Logout + Help
cisco	😽 Contig	Monitor	National Admin			
Virtual Contexts + Operations						
System	Config > Virtual Cont		tificates			1
Load Balancing	🕯 🔍 🖸 💮 🤶 🐑	eb 💌				
	ertificates					🔽 🖬
Certificates	Name	Subject Is	suer	Valid Start Date	Valid End Date	CA Certificate
- Keys				No recorda		
Parameter Map						
Chain Group Parameters						
CSR Parameters						
Proxy Service						
Auth Group Parameters						
Certificate Revocation List						
Security >						
Network 🕨						
High Availability (HA)						
HA Tracking and Failure Detection						
Expert +						
					6	port
Ready					added and a second as	
Ready					Configurations are in sy	nc 04-Aug-2008

- **Step 5** Click **Import...** to import a certificate file. The Import a Certificate/Key File to a Device window reappears. Enter the following parameters. Leave the remaining parameters blank or with their default values.
  - Protocol: FTP
  - IP Address: 172.25.91.100 (in order for this to work, you should use an IP address where you can access the certificate file)
  - Remote Filename: C:\marketing\_cert.pem
  - Local Filename: C:\marketing\_cert.pem
  - Username: Admin

- Password: (password for your FTP server)
- Confirm: (retype the password for your FTP server)
- Step 6 Click OK to import the certificate file.
- Step 7 Choose SSL > Parameter Map. The Parameter Map pane appears (Figure 9-6).

		ACE 4710 Device	Manager A3	(1.0)			Welcome admin	Logout + Help
cisco		🦓 Conta	Monitor	Admin				
Virtual Contexts 👻 Operation	ns							
System		fig > Virtual Contex	ts >SSL >Para	ameter Maj	p			0
Load Balancing		0 0 ? VC_mb	×					
59.	Paran	neter Map						T 🔽 🖬 🚮
- Cetficites		Parameter Map Nam	e Oueue Del	ay Timeout	Session Cache Timeout	Reject Expired CRLs	Close Protocol Behavior	SSL Version
- Keys					No recorda	Treport Deport Data	000000000000000000000000000000000000000	
Parameter Map								
- Chain Group Parameters								
CSR Parameters								
Proxy Service								
<ul> <li>Auth Group Parameters</li> </ul>								
<ul> <li>Certificate Revocation List</li> </ul>								
Security								
Network.								
High Availability (HA)								
HA Tracking and Failure Detection								
Expert								
(	>							
A Ready	_					100	figurations are in sync 04-Au	a.2000

#### Figure 9-6 Parameter Map Pane

Step 8 Click Add to create a parameter map. The Parameter Map window appears (Figure 9-7).

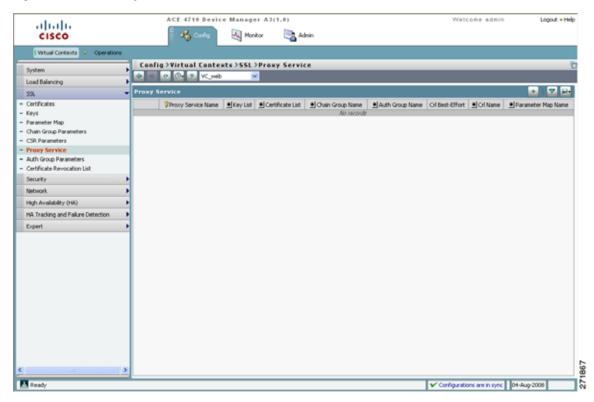
#### Figure 9-7 Parameter Map Window

ahaha	ACE 4710 Device	Manager A3	(1.0)		Welcome adm	in Lo	ogout 🗕 Help
CISCO	Config	Monitor	Carl Admin				
Virtual Contexts 🔹 Operations							
System	Config >¥irtual Co	ntexts >SSL	.≯Parameter Map				Ē
Load Balancing	_ الله الله الله الله ا	dmin	<b>*</b>				
SSL	Parameter Map						
- Certificates	Parameter Map Name* :	PM_SSL_termin	nation				
- Keys	Queue Delay Timeout:						
Parameter Map     Chain Group Parameters	Session Cache Timeout:						
CSR Parameters	Reject Expired CRLs:						
- Proxy Service	Close Protocol Behavior* :	💿 None 🔘	Disabled				
- Auth Group Parameters	SSL Version* :	💽 Ali 🔘 ssi	L3 🔾 TLS1				
Certificate Revocation List     Security	Ignore Authentication Failure	: 🔲					
Network				Deploy Now	Cancel 📢		elete
High Availability (HA)	Parameter Map Cipher						
HA Tracking and Failure Detection	– Parameter Map Cipher @	PM_SSL_termi	ination				
Expert	Cipher Name* : RSA_EX	PORT1024_WITH_	Des_CBC_SHA 🔽				
	Cipher Priority* : 1						
					Deploy Now	Cancel	>*
					500101	Concor	
< >							
	1						100
Ready				<b>√</b> □	M in sync with CLI	04-Aug-2008	

- **Step 9** Enter the following parameter. Leave the remaining parameters blank or with their default values.
  - Parameter Map Name: PM\_SSL\_termination
- Cisco 4700 Series Application Control Engine Appliance Quick Start Guide

- Step 10 Click **Deploy Now** to deploy the parameter map on the ACE appliance. The Parameter Map Cipher pane appears.
- Step 11 Select Add in the Parameter Map Cipher pane (Figure 9-7).
- Step 12 Accept the defaults and click **Deploy Now** in the Parameter Map Cipher pane to add a cipher to the parameter map.
- Step 13 Create an SSL proxy service by choosing SSL > Proxy Service. The Proxy Service pane appears (Figure 9-8).

#### Figure 9-8 Proxy Service Pane



Step 14 Click Add to create a proxy service. The Proxy Service window appears (Figure 9-9).

#### Figure 9-9 Proxy Service Window

ahaha	AGE 4719 Device Manager A3(1.9)	Welcome admin	Logout • Help
cisco	🎝 Conto 🛛 🖓 Monitor 🖓 Admin		
Virtual Contexts   Operations			
System	Config >Virtual Contexts >SSL >Proxy Service		6
Load Balancing	🔹 💿 💿 😰 VC_mb 👻		
59.	Proxy Service		
- Certificates	Proxy Service Name*: P5_S9L_termination		
- Keys	■Key List: ③ N/A		
- Parameter Map	■Certificate List: <ul> <li>N/A</li> </ul>		
<ul> <li>Chain Group Parameters</li> </ul>	Chain Group Name:		
- CSR Parameters	Auth Group Name:		
<ul> <li>Proxy Service</li> <li>Auth Group Parameters</li> </ul>			
<ul> <li>Certificate Revocation List</li> </ul>	Parameter Map Name: O N/A  O PM_SSL_termination		
	<b>x</b>	Deploy Now C	ancel 📴
Network			
High Availability (HA)	•		
HA Tracking and Failure Detection	•		
Expert	•		
	1		
< > >			
Ready	1		kug-2008
Kin Ready		Configurations are in sync 044	AUG-2508

- Step 15 Enter the following parameters. Leave the remaining parameters blank or with their default values.
  - Proxy Service Name: PS\_SSL\_termination
  - Key List: (choose the key file that you imported earlier)
  - Certificate List: (choose the certificate that you imported earlier)
  - Parameter Map Name: PM\_SSL\_termination
- Step 16 Click **Deploy Now** to deploy the proxy service on the ACE appliance.

- Step 17 Configure a virtual server for SSL termination by choosing Load Balancing > Virtual Servers. The Virtual Servers pane appears.
- Step 18 Click Add to create a virtual server. The Add virtual server window appears (Figure 9-10).

Figure 9-10 Add Virtual Server on Virtual Context Window

cisco	ACE 4719 Device Manager A3(1.9) Welcome admin Logo	out • Help
Virtual Contexts + Operations		
System	Config >Virtual Contexts >Load Balancing >Virtual Servers >Add	6
Load Balancing		
Virtual Servers     Real Servers     Real Server Paris     Server Paris     Health Monitoring     Sociales     Parameter Maps     Secure KAL-AP     SSL     Security     Network     High Availability (HA)     HA Tracking and Palure Detection     Expert	Creating Virtual Server on Virtual Context VC_web Bask Wew         ▼           *Properties         ************************************	
<u>s</u>	Server Farm" : SP_web V Verv Dadup Serverfarm: Enable Congression (Deflate Method):	хđ
Ready	✓ Configurations are in sync 04-Aug-2008	

- Step 19 Enter the following parameters. Leave the remaining parameters blank or with their default values.
  - VIP Name: VIP\_SSL
  - VIP IP: 10.10.40.11
  - Protocol: tcp

- Application Protocol: https
- Port: 443
- VLAN: 400
- Proxy Service Name: PS\_SSL\_termination
- Primary Action: loadbalance
- Server Farm: SF\_web

Step 20 Click Deploy Now to deploy the virtual SSL server on the ACE appliance.

## Configuring the ACE for SSL Termination Using the CLI

You can configure the ACE for SSL termination using the CLI by following these steps:

Step 1 Verify that you are operating in the desired context, by checking the CLI prompt. If necessary, change to the correct context.

host1/Admin# changeto VC\_web
host1/VC\_web#

Step 2 Import the key file marketing.pem from an FTP server.

host1/VC\_web# crypto import ftp 172.25.91.100 Admin /marketing.pem
marketing.pem
Password: \*\*\*\*
Passive mode on.
Hash mark printing on (1024 bytes/hash mark).
#
Successfully imported file from remote server.
host1/VC\_web#

**Step 3** Copy the certificate information from the certificate you received from the CA, and paste it into a certificate file called marketing\_cert.pem.

host1/VC\_web# crypto import terminal marketing\_cert.pem

Enter PEM formatted data ending with a blank line or "quit" on a line by itself.

**Step 4** Enter quit to close the file.

**quit** host1/VC\_web#

**Step 5** Verify that the certificate matches the key pair.

host1/VC\_web# crypto verify marketing.pem marketing\_cert.pem
keypair in marketing.pem matches certificate in marketing\_cert.pem

**Step 6** Start configuring SSL termination by entering configuration mode.

host1/VC\_web# config
host1/VC\_web(config)#

Step 7 Create an SSL proxy service.

host1/VC\_web(config)# ssl-proxy service PS\_SSL\_termination
host1/VC\_web(config-ssl-proxy)#

**Step 8** Configure the SSL proxy service by defining the key pair and corresponding certificate.

host1/VC\_web(config-ssl-proxy) # key marketing host1/VC\_web(config-ssl-proxy) # cert marketing\_cert host1/VC\_web(config-ssl-proxy) # exit host1/VC\_web(config) #

Step 9 Create a Layer 3 and Layer 4 class map and configure it with the input traffic match criteria.

```
host1/VC_web(config)# class-map CM_SSL
host1/VC_web(config-cmap)# match virtual-address 10.10.40.11 tcp any
host1/VC_web(config-cmap)# exit
host1/VC_web(config)#
```

Step 10 Create a policy map and associate with it the class map CM\_SSL.

```
host1/VC_web(config)# policy-map multi-match PM_SSL
host1/VC_web(config-pmap)# class CM_SSL
host1/VC_web(config-pmap-c)#
```

**Step 11** Associate the SSL proxy service PS\_SSL\_termination with the policy map.

```
host1/VC_web(config-pmap-c)# ssl-proxy server PS_SSL_termination
host1/VC_web(config-pmap-c)# exit
host1/VC_web(config-pmap)# exit
host1/VC_web(config)#
```

Step 12 Apply the policy map to the input traffic of the VLAN 400 interface.

host1/VC\_web(config)# interface vlan 400
host1/VC\_web(config-if)# service-policy input PM\_SSL

**Step 13** Display the running configuration to verify that the information that you just added is configured properly.

host1/VC\_web(config-if)# do show running-config

In this chapter, you have configured a virtual server for SSL termination. In the next chapter, you will configure server health monitoring.



CHAPTER **10** 

# Configuring Health Monitoring Using Health Probes

This chapter describes how to configure a health probe on the Cisco 4700 Series Application Control Engine (ACE) appliance. This chapter contains the following sections:

- Overview
- Configuring an HTTP Health Probe Using the Device Manager GUI
- Configuring an HTTP Health Probe Using the CLI

### **Overview**

After reading this chapter, you should have a basic understanding of how the ACE appliance supports server health monitoring using health probes, and how to configure an HTTP health probe.

To detect failures and make reliable load-balancing decisions, you can configure the ACE appliance to track the health of servers and server farms by periodically sending out health probes (sometimes referred to as keepalives). By default, the ACE implicitly checks for server failures.

You can configure probes on the ACE to make active connections and explicitly send traffic to servers. The ACE evaluates the server's response to determine the health of that server.

When the ACE determines the health of a server, the result is one of the following:

- Passed—The server returned a valid response.
- Failed—The server failed to provide a valid response to the ACE within a specified number of retries.

When a server fails in response to the probe, the ACE can check for network problems that prevent a client from accessing that server. The ACE can place the server out of service.

A probe can be any of several types, including TCP, UDP, ICMP, Telnet, and HTTP. You can also configure scripted probes using the TCL scripting language.

You can configure a probe by following these steps:

- Step 1 Create the probe and specify its name, type, and attributes.
- **Step 2** Associate the probe with one of the following:
  - A real server.
  - A real server that is associated with a server farm. You can associate a single probe or multiple probes to a real server within a server farm.
  - A server farm. All real servers in the server farm receive the probe.

You can configure a probe by using either the ACE Device Manager GUI or the CLI. This chapter describes how to configure an HTTP probe. For information on how to configure other types of probes, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide.* 

## Configuring an HTTP Health Probe Using the Device Manager GUI

You can configure an HTTP health probe using the ACE Device Manager GUI by following these steps:

Step 1 Choose Load Balancing > Health Monitoring. The Health Monitoring pane appears (Figure 10-1).



abab	ACE 4710 Device Manager A3(1.0)	Welcome admin	Logout • Help
CISCO	🗧 🦓 Config 🛛 🔣 Monitor 🛛 💽 Admin		
Virtual Contexts 👻 Operation	ns		
System	Config >Virtual Contexts >Load Balancing >Health Monit	oring	6
Load Balancing	🗸 🗟 🖉 🖓 ? VC_web 🔽		
- Virtual Servers	Health Monitoring	🔹 i 🔽	🖬 🕘 🔂
- Real Servers	Vame Type Description Probe Interval Pass Detect Count	Pass Detect Interval Receive Timeout	Fail Detect
- Server Farms	No recorda		
<ul> <li>Health Monitoring</li> <li>Stickings</li> </ul>			
<ul> <li>Parameter Maps</li> </ul>			
- Secure KAL-AP			
59.			
Security	•		
Network	•		
High Availability (HA)	•		
HA Tracking and Failure Detection	•		
Expert	•		
<	15		
Ready		✓ Configurations are in sync 01-Aug-2	nne l
Ready		<ul> <li>Comparations are in sync. DP-Aug-2</li> </ul>	000

Step 2 Click Add to add a new health probe. The Health Monitoring window appears (Figure 10-2).

Figure 10-2	Health Monitoring	Window

alada	ACE 4710 De	vice Manager A3	(1.0)	Welcome admin	Logout • Help
cisco	😽 Config	Monitor	Canal Admin		
Virtual Contexts 👻 Operatio	ons				
System			Balancing >Health Monito	ring	0
Load Balancing		VC_web			
- Virtual Servers	Health Monitoring				
- Real Servers	₽Name* :	HTTP_probe1			
<ul> <li>Server Farms</li> </ul>	Type* :	нттр 💌			
<ul> <li>Health Monitoring</li> <li>Stickiness</li> </ul>	Description:				^
<ul> <li>Socialess</li> <li>Parameter Maps</li> </ul>					
<ul> <li>Secure KAL-AP</li> </ul>					
59.	Probe Interval:	5			
Security	Pass Detect Count:	5			
Network					
High Availability (HA)	Pass Detect Interval:	10			
HA Tracking and Failure Detection	Receive Timeout:				
	Fal Detect:				
Expert	Dest IP Address:				
	Is Routed:				
	Port:	80			
	Is Connection:				
	Open Timeout:	10			
	User Name:				
	Password:		Confirm:		
	Expect Regext				
	Expect Regex Offset:				
	Hashc				
	Request Method Type:	O N/A ○Head ○	Get		
<				Deploy Now Ca	ncel 🔽
Ready				<ul> <li>Configurations are in sync</li> <li>01-Ar</li> </ul>	JQ-2008

- **Step 3** Enter the following health probe attributes. Leave the remaining attributes blank or with their default values.
  - Name: HTTP\_probe1
  - Type: HTTP
  - Probe Interval: 5

- Pass Detect Interval: 10
- Port: 80
- Step 4 Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Step 5 Associate the health probe with a server farm by choosing Load Balancing > Server Farms. The Server Farms pane appears (Figure 10-3).

ahaha	ACE 4710 Des	vice Manager A3(1.0)			Welcome admin		Logout • He
CISCO	🔹 🗞 Conto	🛃 Monitor 🛛 🕞	Admin				
Virtual Contexts 🐱 Operations							
System		texts >Load Balancing	Server Farms				_
Load Balancing	🔹 🔍 🔊 💿 🤉 💌	web 💌					
	Server Farms				+ n/ R		B- @ 🔂
Real Servers		None					
Annual Annual	1 () SF_web	VName	Type Host		Description		
Health Monitoring	1 0 SP_Web		Plat				
Richiness							
Parameter Maps							
Secure KAL-AP							
59.							
Security >							
Network +							
High Availability (HA)							
HA Tracking and Falure Detection							
Expert >							
	Real Servers Preditor R	Retrode Map					
1	Real Servers @ SF_web						780
1	Real Servers @ SF_web	ØPort ∎Backup Server	Name Dackup Server Port	Max Connections	Min Connections	Weight	State
	Real Servers @ SF_web	Port ≜Badup Server 80	Name Backup Server Port	4000000	Min Connections 4000000	Weight 8	State In Service
	I         O         R5_web1           2         PS_web2	Port Backup Server	Name Dackup Server Port	4000000	Min Connections 4000000 4000000	Weight 8	State In Service In Service
	Real Servers @ SF_web           ① Name *           1         0           85_web1           2         0           85_web2           3         0	Port Backup Server 80 80 80	Name Backup Server Port	4000000 4000000 4000000	Min Connections 4000000	Weight 8	State In Service In Service
	I         O         R5_web1           2         PS_web2	Port Backup Server	Name Dackup Server Port	4000000	Min Connections 4000000 4000000	Weight 8	State In Service In Service In Service
-	Real Servers @ SF_web           ① Name *           1         0           85_web1           2         0           85_web2           3         0	Port Backup Server 80 80 80	Name Badkup Server Port	4000000 4000000 4000000	Min Connections 4000000 4000000 4000000	Weight 8 8 8	State In Service In Service In Service
-	Real Servers @ SF_web           ① Name *           1         0           85_web1           2         0           85_web2           3         0	Port Backup Server 80 80 80	Name Backup Server Port	4000000 4000000 4000000	Min Connections 4000000 4000000 4000000	Weight 8 8 8	State In Service In Service In Service
	Real Servers @ SF_web           ① Name *           1         0           85_web1           2         0           85_web2           3         0	Port Backup Server 80 80 80	Name Backup Server Port	4000000 4000000 4000000	Min Connections 4000000 4000000 4000000	Weight 8 8 8	State In Service In Service In Service
	Real Servers @ SF_web           ① Name *           1         0           85_web1           2         0           85_web2           3         0	Port Backup Server 80 80 80	Name Dadup Server Port	4000000 4000000 4000000	Min Connections 4000000 4000000 4000000	Weight 8 8 8	State In Service In Service In Service
	Real Servers @ SF_web           ① Name *           1         0           85_web1           2         0           85_web2           3         0	Port Backup Server 80 80 80	Name Backup Server Port	4000000 4000000 4000000	Min Connections 4000000 4000000 4000000	Weight 8 8 8	State In Service In Service In Service
	Real Servers @ SF_web           ① Name *           1         0           85_web1           2         0           85_web2           3         0	Port Backup Server 80 80 80	Name Backup Server Port	4000000 4000000 4000000	Min Connections 4000000 4000000 4000000	Weight 8 8 8	State In Service In Service In Service
	Real Servers @ SF_web           ① Name *           1         0           85_web1           2         0           85_web2           3         0	Port Backup Server 80 80 80	Name Backup Server Port	4000000 4000000 4000000 4000000	Min Connections 4000000 4000000 4000000	Weight 8 8 8 8 8 8 8	State In Service In Service In Service

Figure 10-3 Server Farms Pane

Step 6 Choose the server farm SF\_web and click Edit. The Server Farms window appears (Figure 10-4).



de de	ACE 4710 De	vice Manager A3(1	1.0)			Welcome admin		Logout • Help
cisco	🛛 🔩 Contra	Monitor	Radmin 🔁					
Virtual Contexts + Operations								
System	Config > Virtual Con		ncing >Serv	er Farms				0
Load Balancing		web 💌						
- Virtual Servers	- Server Farms							
- Real Servers	%Name*:	SF_web						
- Server Farms	Type* :	Host      Redrect						
<ul> <li>Health Monitoring</li> </ul>	Description:							0
- Stickiness								
<ul> <li>Parameter Maps</li> </ul>								
<ul> <li>Secure KAL-AP</li> <li>SSL</li> </ul>								19
	Pal Action:	⊙ N/A ○Purge						
Security	Transparent:	O AØA ⊙False ⊙Tr	ue					
Network	Partial-threshold Percentage:	0						
High Availability (HA)	Back Inservice:	0						
HA Tracking and Falure Detection	Probes:	Available Items Sel	ected Items					
Dpert	, -		TTP_probe1					
		9						
					Deploy Now	Carcel		Delete
	Real Servers (4 Reses) Pre	edictor (1 Rese) Retords Ma	w					
	Real Servers @ SF_meb					🔹 🖸		7 H- @
	🕐 🕅 🕐 Name 🔻	Port Backup 1	Server Name	Backup Server Port	Max Connections	Min Connections	Weight	Sate
	1 O R5_web1	80			4000000	4000000	0	In Service
	2 O R5_web2	80			4000000	4000000	8	In Service
	3 R5_web3	80			4000000	4000000		In Service
	4 O R5_web4	80			4000000	4000000	8	In Service
<	>							
Ready					✓ Corb	purations are in sync	04-Aug-20	008

- Step 7 For Probes, choose HTTP\_probe1 from the Available Items list, and click the right-arrow button to move the probe to the Selected Items list.
- Step 8 Click **Deploy Now** to associate the health probe HTTP\_probe1 with the server farm SF\_web.

### Configuring an HTTP Health Probe Using the CLI

You can configure an HTTP health probe using the CLI by following these steps:

Step 1 Verify that you are operating in the desired context by checking the CLI prompt. If necessary, change to the correct context.

host1/Admin# changeto VC\_web
host1/VC\_web#

**Step 2** Enter configuration mode.

host1/VC\_web# config host1/VC\_web(config)#

**Step 3** Define an HTTP probe named HTPP\_probe1 to access its configuration mode.

host1/VC\_web(config)# probe http HTTP\_probe1
host1/VC\_web(config-probe-http)#

Step 4 Configure port number 80 for the HTTP probe.

host1/VC\_web(config-probe-http)# port 80

**Step 5** Configure a time interval of 5 seconds between probes.

host1/VC\_web(config-probe-http)# interval 5

Step 6 Configure a pass detect interval of 10 seconds, after which the ACE will send another probe to a failed server.

host1/VC\_web(config-probe-http)# passdetect interval 10

**Step 7** Exit probe configuration mode.

host1/VC\_web(config-probe-http)# exit
host1/VC\_web(config)#

**Step 8** Associate the probe HTTP\_probe1 with the server farm SF\_web, and exit configuration mode.

```
host1/VC_web(config)# serverfarm SF_web
host1/VC_web(config-sfarm-host)# probe HTTP_probe1
host1/VC_web(config-sfarm-host)# exit
host1/VC_web(config)# exit
host1/VC_web#
```

Step 9 Display the HTTP probe configuration. host1/VC\_web# show running-config probe

In this chapter, you have configured an HTTP health probe.

Cisco 4700 Series Application Control Engine Appliance Quick Start Guide



#### ΙΝΟΕΧ

#### Α

access control lists. *See* ACLs ACLs 4-1 Address Resolution Protocol. *See* ARP Admin context 3-2 Admin role 5-2 ARP 3-23

#### С

CA 9-2

certificate authority. *See* CA certificate signing request. *See* CSR ciphertext 9-3 class map 6-13, 9-5 clear text 5-10, 9-3 CLI 2-1, 2-9, 2-21 client requests stuck to a server figure 8-4 client-side VLAN interface 3-12, 3-26 command-line interface. *See* CLI configuring the client-side VLAN interface figure 3-12 configuring the server-side VLAN interface figure 3-16
console 2-4
cookies 8-2
creating a user context figure 3-7
CSR 9-2

#### D

Device Manager. *See* GUI digital certificates 9-2 domain 5-1

#### Ε

encryption 5-10, 9-2 Ethernet interface 2-4, 2-19, 2-22, 2-26, 2-27 figure 2-15 example network setup figure 2-2

#### G

graphical user interface. *See* GUI GUI 2-1, 2-9, 2-12

#### Η

health probes 10-1 high availability 1-2, 1-3

#### L

load-balancing predictor 7-1

#### Μ

MAC 3-23 management VLAN interface 2-25, 3-23 Media Access Control. *See* MAC mega-proxy 8-2

#### Ν

NAT **3-16** network address translation. *See* NAT

#### Ρ

persistence 8-1 PKI 9-1 policy map 6-13 predictor 7-1 types of 7-2 private key 9-2 probes 10-1 types of 10-2 public key 9-2 public key infrastructure. *See* PKI

#### R

RBAC 5-1 real servers 6-1, 6-2 remote management access 2-27 resource classes 3-2 Role-Based Access Control. *See* RBAC roles 5-2

#### S

scalability 1-2, 1-3 table 1-5 secure sockets layer. *See* SSL security 1-2, 1-3 server farm 6-2 server load balancing 1-2, 6-1 figure 6-2 server persistence 8-1 server-side VLAN interface 3-16, 3-27 session 8-2 setup script 2-8 SSL 1-3, 9-1 SSL configurations

Cisco 4700 Series Application Control Engine Appliance Quick Start Guide

end-to-end 9-4 figure 9-3 initiation 9-3 termination 9-3 SSL proxy service 9-2, 9-5 stickiness 8-2 sticky groups 8-3 methods 8-2 table 8-3

#### Т

Telnet access 2-30 traffic policy 6-13

#### U

user context 3-7 user roles 5-2

#### V

VIP 6-1 virtual contexts 3-2 virtualization 3-1, 3-2 virtual local area network. *See* VLAN virtual server. *See* VIP VLAN 2-3 Index