



# Preface

---

This guide describes how to configure the security feature of the Cisco Application Control Engine (ACE) module or a Cisco 7600 series router, hereinafter referred to as the switch or router, respectively.

This guide describes how to perform the following ACE security configuration tasks:

- Security access control lists (ACLs)
- 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 IP fragmentation
- Network Address Translation (NAT)

This preface contains the following major sections:

- [Audience](#)
- [How to Use This Guide](#)
- [Related Documentation](#)
- [Symbols and Conventions](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)
- [Notices](#)

# 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   |
|--|---|
| <a href="#">Chapter 1, Configuring Security Access Control Lists</a>                     | Describes how to configure security access control lists (ACLs) on your ACE. ACLs provide basic security for your network by filtering traffic and controlling network connections. |
| <a href="#">Chapter 2, Configuring Authentication and Accounting Services</a>            | Describes how to configure the ACE to perform user authentication and accounting (AAA) services. These services provide a higher level of security for users who access the ACE.    |
| <a href="#">Chapter 3, Configuring Application Protocol Inspection</a>                   | Describes application protocol inspection and how to configure it on the ACE.   |
| <a href="#">Chapter 4, Configuring TCP/IP Normalization and IP Reassembly Parameters</a> | Describes TCP/IP normalization and how to configure it to protect your ACE and the data center from attacks. It also describes IP reassembly and UDP parameters.                    |
| <a href="#">Chapter 5, Configuring Network Address Translation</a>                       | Describes NAT and how to configure it on the ACE. NAT protects your data center by hiding private addresses from public networks.   |

# Related Documentation

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

| <b>Document Title</b>   | <b>Description</b>   |
|---|--|
| <i>Release Note for the Cisco Application Control Engine Module</i>               | Provides information about operating considerations, caveats, and command-line interface (CLI) commands for the ACE.   |
| <i>Cisco Application Control Engine Module Hardware Installation Note</i>         | Provides information for installing the ACE into the Catalyst 6500 series switch or a Cisco 7600 series router.  |
| <i>Cisco Application Control Engine Module Getting Started Guide</i>              | Describes how to perform the initial setup and configuration tasks for the ACE.  |
| <i>Cisco Application Control Engine Module Administration Guide</i>               | Describes how to perform the following administration tasks on the ACE: <ul style="list-style-type: none"> <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> |
| <i>Cisco Application Control Engine Module Virtualization Configuration Guide</i> | Describes how to operate your ACE in a single context or in multiple contexts.   |

| <b>Document Title</b>  | <b>Description</b>  |
|--|---|
| <i>Cisco Application Control Engine Module Routing and Bridging Configuration Guide</i>  | <p>Describes how to configure the following routing and bridging features on the ACE:</p> <ul style="list-style-type: none"> <li>• VLAN interfaces</li> <li>• Routing</li> <li>• Bridging</li> <li>• Dynamic Host Configuration Protocol (DHCP)</li> </ul>  |
| <i>Cisco Application Control Engine Module Server Load-Balancing Configuration Guide</i> | <p>Describes how to configure the following server load-balancing features on the ACE:</p> <ul style="list-style-type: none"> <li>• Real servers and server farms</li> <li>• Class maps and policy maps to load balance traffic to real servers in server farms</li> <li>• Server health monitoring (probes)</li> <li>• Stickiness</li> <li>• Firewall load balancing</li> <li>• TCL scripts</li> </ul> |
| <i>Cisco Application Control Engine Module SSL Configuration Guide</i>                   | <p>Describes how to configure the following Secure Sockets Layer (SSL) features on the ACE:</p> <ul style="list-style-type: none"> <li>• SSL certificates and keys</li> <li>• SSL initiation</li> <li>• SSL termination</li> <li>• End-to-end SSL</li> </ul>  |
| <i>Cisco Application Control Engine Module System Message Guide</i>                      | <p>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.</p>   |
| <i>Cisco Application Control Engine Module Command Reference</i>                         | <p>Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.</p>   |

| Document Title                                     | Description  |
|--|--|
| <i>Cisco CSM-to-ACE Conversion Tool User Guide</i> | Describes how to use the CSM-to-ACE conversion tool to migrate Cisco Content Switching Module (CSM) running- or startup-configuration files to the IM. |
| <i>Cisco CSS-to-ACE Conversion Tool User Guide</i> | Describes how to use the CSS-to-IM conversion tool to migrate Cisco Content Services Switches (CSS) running- or startup-configuration files to the IM. |

## 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.                                       |
| <i>italic</i> font   | Arguments for which you supply values are in <i>italics</i> . Italic text also indicates the first occurrence of a new term, book title, emphasized text. |
| { }                  | Encloses required arguments and keywords.   |
| [ ]                  | Encloses optional arguments and keywords.   |
| { x   y   z }        | Required alternative keywords are grouped in braces and separated by vertical bars.   |
| [ 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 <code>screen font</code> .   |

| Convention                  | Description  |
|-----------------------------|--|
| <b>boldface screen font</b> | Information you must enter in a command line is in <b>boldface screen font</b> .   |
| <i>italic screen font</i>   | Arguments for which you supply values are in <i>italic screen font</i> .   |
| ^                           | 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.   |

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:



**Caution**

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

For additional information about CLI syntax formatting, see the *Cisco Application Control Engine Module Command Reference*.

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

## 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](mailto: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](mailto:openssl-core@openssl.org).
5. 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].