# はじめに

このマニュアルでは、Cisco 4700 Series Application Control Engine（ACE）アプライアンスのセキュリティ機能の設定方法について説明します。

また、以下の ACE のセキュリティ設定タスクの実行方法についても説明します。

- セキュリティ アクセス コントロールリスト（ACL）
- Terminal Access Controller Access Control System Plus（TACACS+）、または Remote Authentication Dial-In User Service（RADIUS）、または Lightweight Directory Access Protocol（LDAP）サーバを使用したユーザ認証およびアカウンティング
- アプリケーション プロトコルおよび HTTP ディープ パケット インスペクション
- TCP/IP 正規化および IP フラグメンテーション
- ネットワーク アドレス変換（NAT）

次のインターフェイスを使用して ACE を設定できます。

- コマンドライン インターフェイス（CLI）- ACE の設定、管理、および監視用のコマンドを提供する行指向のユーザ インターフェイス
- デバイス マネージャ GUI - ACE の設定、管理、および監視用のグラフィカル ユーザ インターフェイスを提供する Web ブラウザ ベースの GUI インターフェイス

ここで説明する主な内容は次のとおりです。

# 対象読者

このマニュアルでは、ACE 設定の責任者で、トレーニングを受けて十分な知識を持つ次のような担当者を対象読者としています。

- Web マスター
- システム管理者
- システム運用担当者

# このマニュアルの利用方法

このマニュアルは次の章で構成されています。

| 章 | 説明 |
|---|---|
| 第 1 章 セキュリティ アクセス コントロール リストの設定 | ACE のセキュリティ アクセス コントロール リスト（ACL）を設定する方法を説明します。ACL を利用すると、トラフィックに対するフィルタリングやネットワーク接続の制御を行うことが可能で、ネットワークに基本的セキュリティを与えることができます。 |
| 第 2 章 認証サービスおよびアカウンティング サービスの設定 | ユーザ認証およびアカウンティング（AAA）サービスを実行し、ACE にアクセスするユーザにレベルの高いセキュリティを提供するための ACE の設定方法について説明します。 |
| 第 3 章 アプリケーション プロトコル インスペクションの設定 | ACE のアプリケーション プロトコル インスペクションの設定方法について説明します。 |
| 第 4 章 TCP/IP 正規化パラメータおよび IP 再構成パラメータの設定 | ACE とデータセンターを攻撃から守るための TCP/IP 正規化の設定方法について説明します。また、IP の再構成と UDP パラメータについても説明します。 |
| 第 5 章 NAT の設定 | NAT および、ACE でのその設定方法を説明します。NAT はプライベート アドレスを公開ネットワークから隠蔽することにより、データセンターを保護します。 |

# 関連資料

このマニュアルの他にも、ACE の資料として次のものが用意されています。

| 資料の名称 | 説明 |
|---|---|
| *Release Note for the Cisco Application Control Engine Module* | 操作上の留意点、警告、ACE 用のコマンドライン インターフェイス（CLI）に関する情報を提供しています。 |
| *Cisco Application Control Engine Appliance Hardware Installation Guide* | ACE アプライアンスのインストールに関する情報を記載しています。 |
| *Regulatory Compliance and Safety Information for the Cisco Application Control Engine Appliance* | ACE アプライアンスの適合規格および安全性に関する情報を記載しています。 |
| *Cisco 4700 Series Application Control Engine Appliance Quick Start Guide* | ACE アプライアンスでデバイス マネージャおよび CLI を使用して、初期設定および VIP ロード バランシングの設定を行う方法を記載しています。 |
| *Cisco 4700 Series Application Control Engine Appliance Administration Guide* | ACE 上で次の管理作業を行う方法について説明しています。<br>• ACE のセットアップ<br>• リモート アクセスの設定<br>• ソフトウェア ライセンスの管理<br>• クラス マップとポリシー マップの設定<br>• ACE ソフトウェアの管理<br>• SNMP の設定<br>• 冗長性の設定<br>• XML インターフェイスの設定<br>• ACE ソフトウェアのアップグレード |

| 資料の名称 | 説明 |
|---|---|
| *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide* | 単一コンテキストまたは複数コンテキストで ACE を運用する方法を説明しています。 |
| *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide* | ACE で次のルーティングおよびブリッジングに関する作業を行う方法について説明します。<br>• イーサネット ポートの設定<br>• VLAN インターフェイスの設定<br>• ルーティングの設定<br>• ブリッジングの設定<br>• Dynamic Host Configuration Protocol（DHCP）の設定 |
| *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide* | 次に挙げる ACE のサーバ ロード バランス機能を設定する方法を説明しています。<br>• 実サーバとサーバ ファーム<br>• サーバ ファーム内の実サーバへのトラフィックをロード バランシングするためのクラス マップとポリシー マップ<br>• サーバ ヘルス モニタリング（プローブ）<br>• スティッキ性<br>• ファイアウォール ロード バランシング<br>• TCL スクリプト |
| *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide* | ACE の Web 最適化機能の設定方法を説明しています。また、これら機能の概要および説明も提供します。 |

| 資料の名称 | 説明 |
|---|---|
| *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide* | 次に挙げる ACE の SSL（Secure Sockets Layer）機能を設定する方法を説明しています。<br>• SSL 認証と暗号キー<br>• SSL の始動<br>• SSL の停止<br>• エンドツーエンド SSL |
| *Cisco 4700 Series Application Control Engine Appliance System Message Guide* | ACE のシステム メッセージ ロギングを設定する方法を説明します。このマニュアルには、ACE で生成される syslog メッセージの一覧と説明も含まれています。 |
| *Cisco 4700 Series Application Control Engine Appliance Command Reference* | CLI の全コマンドをアルファベット順に記載し、モード、構文、オプション、関連コマンドなどを説明しています。 |
| *Cisco 4700 Series Application Control Engine Appliance Device Manager GUI Configuration Guide* | ACE のフラッシュ メモリ上に常駐しているデバイス マネージャ GUI を使用して、アプライアンスを設定および管理するためのブラウザ ベース インターフェイスを提供する方法について説明します。 |
| *Cisco CSS-to-ACE Conversion Tool User Guide* | Cisco Content Services Switches（CSS）から ACE への変換ツールを使用して、CCS の実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを ACE に移行する方法について説明します。 |

# 表記法について

このマニュアルでは、次の表記法を使用しています。

| 表記法 | 説明 |
|---|---|
| **太字** | コマンド、コマンド オプション、およびキーワードは**太字**で示しています。本文の中のコマンドも太字で示します。 |
| *イタリック体* | ユーザが値を指定する引数は、*イタリック体*で示しています。また、始めて現れた新しい用語、資料名、強調部分もイタリックで示します。 |
| { } | 必要な引数とキーワードを示します。 |
| [ ] | 任意でよい引数とキーワードを示します。 |
| { x \| y \| z } | 必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。 |
| [ x \| y \| z ] | どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。 |
| ストリング | 引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。 |
| `screen` フォント | システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。 |
| **太字の `screen` フォント** | ユーザがコマンド ラインに入力しなければならない情報は、**太字の `screen` フォント**で示しています。 |
| *イタリック体の screen フォント* | ユーザが値を指定する引数は、*イタリック体の screen* フォントで示しています。 |
| ^ | ^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。 |
| < > | パスワードのように出力されない文字は、かぎカッコ（< >）で囲んで示しています。 |

（注）は、次のように表しています。

**（注）** 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意は、次のように表しています。

**注意** 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

CLI の構文形式についての追加情報は『*Cisco 4700 Series Application Control Engine Appliance Command Reference*』を参照してください。

# マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

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

# オープン ソース ライセンス通知

本ソフトウェア ライセンスには、次の承認事項が適用されます。

# 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:



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.
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:

© 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].