はじめに

このマニュアルでは、Cisco Application Control Engine（ACE）モジュールまたは Cisco 7600 シリーズ ルータのセキュリティ機能を設定する方法について説明します。ここでは前者を「スイッチ」、後者を「ルータ」と呼びます。

また、以下の ACE のセキュリティの設定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）

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」	ACE を設定して、ユーザ認証およびアカウンティング（AAA）サービスを実行する方法について説明します。これらのサービスにより、ACE にアクセスするユーザに高度なレベルのセキュリティが提供されます。
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」	アプリケーション プロトコル インスペクションおよび、ACE でのそ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」	TCP/IP の正規化について説明し、ACE およびデータセンターを攻撃から保護するための設定方法を説明します。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 Module Hardware Installation Note*』	Catalyst 6500 シリーズ スイッチ、または Cisco 7600 シリーズ ルータへの ACE のインストールに必要な情報を示します。
『*Cisco Application Control Engine Module Getting Started Guide*』	ACE で行う初期のセットアップ、および構成作業の実行方法について説明します。
『*Cisco Application Control Engine Module 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。 • ACE のセットアップ • リモート アクセスの設定 • ソフトウェア ライセンスの管理 • クラス マップとポリシー マップの設定 • ACE ソフトウェアの管理 • SNMP の設定 • 冗長性の設定 • XML インターフェイスの設定 • ACE ソフトウェアのアップグレード
『*Cisco Application Control Engine Module 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。

資料の名称	説明
『*Cisco Application Control Engine Module Routing and Bridging Configuration Guide*』	ACE で次のルーティングとブリッジングの機能を設定する方法について説明しています。 • VLAN インターフェイス • ルーチング • ブリッジング • DHCP（Dynamic Host Configuration Protocol）
『*Cisco Application Control Engine Module 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。 • 実サーバとサーバ ファーム • 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 • サーバ ヘルス モニタリング（プローブ） • スティッキ性 • ファイアウォール ロード バランシング • TCL スクリプト
『*Cisco Application Control Engine Module 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。 • SSL 認証と暗号キー • SSL の始動 • SSL の停止 • エンドツーエンド SSL
『*Cisco Application Control Engine Module 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。また、ACE が生成するシステム ログ（Syslog）メッセージの一覧と解説も記載しています。
『*Cisco Application Control Engine Module 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。

資料の名称	説明
『*Cisco CSM-to-ACE Conversion Tool User Guide*』	Cisco Content Switching Module（CSM）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 ファイルから IM への移行に利用する CSM/ACE 変換ツールの使い方を説明しています。
『*Cisco CSS-to-ACE Conversion Tool User Guide*』	Cisco Content Services Switches（CSS）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 ファイルから IM へ移行するために利用する CSM/IM 変換ツールの使い方を説明しています。

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	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 }	必ずどれか 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 Application Control Engine Module Command Reference*』を参照してください。

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手、テクニカル サポート、マニュアルに関するフィードバック、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコ製品のマニュアルの詳細については、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。この参照情報には、シスコの新規および改訂版の技術マニュアルの一覧が記載されています。

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

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

オープン ソース ライセンスの承認

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:

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.

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].