セキュリティ機能の設定

この章では、Cisco 1800 サービス統合型固定構成ルータで設定可能な特定のセキュリティ機能を実装するシスコの主要なフレームワークである、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）の概要について説明します。

（注） ルータの各モデルは、このマニュアルに記載されている機能の一部をサポートしていない場合があります。特定のルータでサポートされていない機能は、可能な限り明示されています。

この章で説明する内容は、次のとおりです。

- 「認証、許可、アカウンティング」
- 「AutoSecure の設定」
- 「アクセス リストの設定」
- 「CBAC ファイアウォールの設定」
- 「Cisco IOS Firewall IDS の設定」
- 「VPN の設定」

該当する場合、各項には設定例と確認手順が記載されています。

認証、許可、アカウンティング

AAA のネットワーク セキュリティ サービスは、ルータ上でアクセス制御を設定する主要なフレームワークを提供します。認証は、ログインおよびパスワード ダイアログ、確認要求および応答、メッセージングのサポート、暗号化（選択するセキュリティ プロトコルに応じて）など、ユーザを識別するための方法を提供します。許可は、1 回限りの許可や各サービスに対する許可、各ユーザに対するアカウント リストおよびプロファイル、ユーザ グループのサポート、IP、Internetwork Packet Exchange（IPX; インターネットワーク パケット交換）、AppleTalk Remote Access（ARA; AppleTalk リモート アクセス）、および Telnet のサポートなど、リモート アクセスを制御するための方法を提供します。アカウンティングは、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、バイト数など、課金、監査、およびレポートに使用するセキュリティ サーバ情報を収集し、送信するための方法を提供します。

AAA は RADIUS、TACACS+、または Kerberos などのプロトコルを使用してセキュリティ機能を管理します。ルータがネットワーク アクセス サーバとして機能している場合、AAA は、ネットワーク アクセス サーバと RADIUS、TACACS+、または Kerberos セキュリティ サーバ間の通信を確立するための手段となります。

AAA サービスおよびサポートされているセキュリティ プロトコルの設定については、『*Cisco IOS Security Configuration Guide*』の次の項を参照してください。

- 認証の設定
- 「Configuring Authorization」
- 「Configuring Accounting」
- 「Configuring RADIUS」
- 「Configuring TACACS+」
- 「Configuring Kerberos」

AutoSecure の設定

AutoSecure 機能は、ネットワーク攻撃に悪用される可能性のある一般的な IP サービスをディセーブルにし、攻撃を受けたときはネットワークの防御に役立つ IP サービスおよび機能をイネーブルにできます。この IP サービスは、1 つのコマンドですべてを同時にディセーブル/イネーブルにすることにより、ルータ上のセキュリティ設定を大幅に簡易化しています。AutoSecure 機能の詳細については、『AutoSecure』機能マニュアルを参照してください。

アクセス リストの設定

アクセス リスト（ACL）は、送信元 IP アドレス、宛先 IP アドレス、またはプロトコルに基づいてインターフェイス上でネットワーク トラフィックの許可または拒否を行います。アクセス リストは、標準版または拡張版のどちらかに設定されます。標準アクセス リストは、指定された送信元からのパケットの通過を許可または拒否します。拡張アクセス リストでは、宛先および送信元の両方を指定できます。また、各プロトコルを指定して、通過を許可または拒否することができます。アクセス リストは、一般的なタグによってコマンドがバインドされる一連のコマンドです。タグは、番号または名前のどちらかです。表 12-1 は、アクセス リストの設定に使用するコマンドのリストです。

表 12-1　アクセス リストのコンフィギュレーション コマンド

ACL タイプ	コンフィギュレーション コマンド
番号形式	
標準	**access-list** {**1-99**}{**permit** | **deny**} *source-addr* [*source-mask*]
拡張	**access-list** {**100-199**}{**permit** | **deny**} *protocol source-addr* [*source-mask*] *destination-addr* [*destination-mask*]
名前形式	
標準	**ip access-list standard** *name* followed by **deny** {*source* | *source-wildcard* | **any**}
拡張	**ip access-list extended** *name* followed by {**permit** | **deny**} *protocol* {*source-addr* [*source-mask*] | **any**}{*destination-addr* [*destination-mask*] | **any**}

アクセス グループ

一般的な名前または番号にバインドされている一連のアクセス リストの定義をアクセス グループと呼びます。アクセス グループは、インターフェイスの設定時に次のコマンドを使用すると、インターフェイスに対してイネーブルになります。

ip access-group *number* | *name* [**in** | **out**]

ここで、**in** | **out** は、フィルタリングされるパケットの伝送方向を指します。

アクセス グループの作成に関する注意事項

アクセス グループを作成する際には、次の点に注意します。

- アクセス リストの定義の順序は重要です。パケットは、最初のアクセス リストから順に照合されます。一致するものがない場合（つまり、許可または拒否が発生しない場合）は、次のアクセス リストに照合され、さらに次のアクセス リストへと順に進められます。
- パケットが許可または拒否される前に、すべてのパラメータがアクセス リストに一致する必要があります。
- すべてのシーケンスの末尾には、暗黙の「deny all」が付きます。

アクセス リストの作成の詳細については、『*Cisco IOS Release 12.3 Security Configuration Guide*』の「Access Control Lists: Overview and Guidelines」を参照してください。

CBAC ファイアウォールの設定

Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）では、ステートフルなファイアウォールを設定できます。ステートフルなファイアウォールでは、パケットが内部的に検査され、ネットワーク接続の状態がモニタされます。これは、スタティックなアクセス リストよりも優れています。なぜならアクセス リストは、パケットのストリームではなく、個別のパケットに基づいてトラフィックの許可または拒否のみを実行するためです。また、CBAC はパケットの検査を行うため、アプリケーション レイヤのデータを調べてトラフィックの許可または拒否を判断できます。スタティックなアクセス リストでは、このような検査を行うことはできません。

CBAC ファイアウォールを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用して、検証するプロトコルを指定します。

ip inspect name *inspection-name protocol* **timeout** *seconds*

指定したプロトコルがファイアウォールを通過していることがインスペクションで検出された場合、ダイナミック アクセス リストが作成され、リターン トラフィックの通過を許可します。**timeout** パラメータでは、ルータを通過する戻りトラフィックが存在しない場合にダイナミック アクセス リストをアクティブにしておく時間を指定します。タイムアウト値が指定値に達すると、ダイナミック アクセス リストが削除され、後続のパケット（有効なパケットの場合もある）が許可されなくなります。

複数のステートメントで同一のインスペクション名を使用して、1 つのルール セットにまとめてください。ファイアウォールにインターフェイスを設定するときに、**ip inspect** *inspection-name* **in** | **out** コマンドを使用して、このルール セットを設定の別の場所でアクティブ化できます。

サンプル設定については、第 8 章「簡易ファイアウォール」を参照してください。CBAC ファイアウォールの設定の詳細については、『*Cisco IOS Release 12.3 Security Configuration Guide*』の「Configuring Context-Based Access Control」を参照してください。

Cisco IOS Firewall IDS の設定

Cisco IOS Firewall Intrusion Detection System（IDS; 侵入防御システム）テクノロジーは、セキュリティ ポリシーに違反したり悪意のあるネットワーク アクティビティを表したりするパケットおよびフローを適切に処理することで、境界ファイアウォール保護を強化します。

Cisco IOS Firewall IDS は、「シグニチャ」を使用してネットワーク トラフィックから悪用のパターンを検出することで、最も一般的な 59 種類の攻撃を識別します。また、インライン型の侵入検知装置として機能し、ルータを通過するパケットおよびセッションをモニタして、いずれかの IDS シグニチャとの比較を行います。疑わしいアクティビティを検出すると、ネットワーク セキュリティが損害を受ける前に対応し、イベントを記録し、設定に応じてアラームを送信するか、疑いのあるパケットをドロップするか、または TCP 接続をリセットします。

Cisco IOS Firewall IDS の設定の詳細については、『*Cisco IOS Release 12.3 Security Configuration Guide*』の「Configuring Cisco IOS Firewall Intrusion Detection System」を参照してください。

VPN の設定

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）接続を使用すると、インターネットなどのパブリック ネットワーク上で 2 つのネットワーク間のセキュアな接続を実現できます。Cisco 1800 シリーズの固定構成アクセス ルータは、IP Security（IPSec; IP セキュリティ）トンネルおよび Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）を使用してサイト間 VPN をサポートします。2 つのピア間の永続的な VPN 接続、または、必要に応じて VPN 接続を作成および切断する EZVPN または DMVPN を使用した動的な VPN を設定できます。第 6 章「Easy VPN および IPSec トンネルを使用した VPN の設定」と第 7 章「IPSec トンネルと汎用ルーティング カプセル化を使用した VPN の設定」に、これらの機能を使用したルータの設定例を示しています。IPSec および GRE の設定の詳細については、『*Cisco IOS Release 12.3 Security Configuration Guide*』の「Configuring IPSec Network Security」を参照してください。

Cisco 1800 シリーズの固定構成アクセス ルータがサポートするその他の VPN 設定については、次の機能マニュアルを参照してください。

- 『VPN Access Control Using 802.1X Authentication』: 802.1x 認証の使用により、社員が企業ネットワークに自宅からアクセスでき、一方でリモート テレワーカー本人以外の家族はインターネットのみにアクセスできるようになります。
- 『EZVPN Server』: Cisco 1800 シリーズ固定構成ルータは、EZVPN サーバとして機能するように設定できます。これによって、許可された EZVPN クライアントは、接続しているネットワークへの動的な VPN トンネルを確立できるようになります。
- 『Dynamic Multipoint VPN (DMVPN)』: DMVPN 機能により、必要に応じてマルチポイント構成の複数のルータ間に VPN トンネルを作成でき、設定が簡素化され、永続的なポイントツーポイント VPN トンネルの必要がなくなります。