CHAPTER 32

AAA について

この章では、認証、許可、アカウンティング（AAA は「トリプル A」と読む）について説明します。AAA は、コンピュータ リソースへのアクセスを制御するための一連のサービスで、サービスの課金に必要な情報を提供します。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

この章は、次の項で構成されています。

認証

認証はユーザを特定する方法です。アクセスが許可されるには、ユーザは通常、有効なユーザ名と有効なパスワードが必要です。AAA サーバは、データベースに保存されている他のユーザ クレデンシャルとユーザの認証資格情報を比較します。クレデンシャルが一致する場合、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合、認証は失敗し、ネットワーク アクセスは拒否されます。

次の項目を認証するように、ASA を設定できます。

- ASA へのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH。詳細については、第 45 章「管理アクセスの設定」を参照してください。
  - シリアル コンソール
  - ASDM（HTTPS を使用）
  - VPN 管理アクセス
- **enable** コマンド 詳細については、第 45 章「管理アクセスの設定」を参照してください。

- ネットワーク アクセス 詳細については、Chapter 47, “Configuring AAA Rules for Network Access,”、第 39 章「Cisco TrustSec と統合するための ASA の設定」、および第 38 章「アイデンティティ ファイアウォールの設定」を参照してください。
- VPN アクセス 詳細については、Chapter 6, “Configuring Remote Access IPsec VPNs,”、Chapter 8, “Configuring Easy VPN Services on the ASA 5505,”、およびChapter 10, “Configuring LAN-to-LAN IPsec VPNs,” を参照してください。Chapter 78, “Configuring Clientless SSL VPN.”

許可

承認はポリシーを使用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザが持っているのかを判断します。ユーザが認証されると、そのユーザは別のタイプのアクセスまたはアクティビティが承認される可能性があります。

次の項目を許可するように、ASA を設定できます。

- 管理コマンド 詳細については、第 45 章「管理アクセスの設定」を参照してください。
- ネットワーク アクセス 詳細については、Chapter 47, “Configuring AAA Rules for Network Access.” を参照してください。
- VPN アクセス 詳細については、Chapter 6, “Configuring Remote Access IPsec VPNs,”、Chapter 8, “Configuring Easy VPN Services on the ASA 5505,”、およびChapter 10, “Configuring LAN-to-LAN IPsec VPNs,” を参照してください。Chapter 78, “Configuring Clientless SSL VPN.”

Accounting

アカウンティングは、アクセス時にユーザが消費したリソースを測定します。そこには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウンティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティ プランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、許可、アカウンティング間の相互作用

認証だけで使用することも、許可およびアカウンティングとともに使用することもできます。許可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および許可とともに使用することもできます。

AAA サーバ

AAA サーバはアクセス コントロールに使用されるネットワーク サーバです。認証は、ユーザを識別します。承認はどのリソース認証ユーザをアクセスするかもしれない保守するかを指定するポリシーを実行します。アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。

AAA サーバ グループ

認証、許可、またはアカウンティングに外部 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの AAA サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバ グループは名前で識別されます。各サーバ グループは、あるサーバまたはサービスに固有です。

ローカル データベースのサポート

ASA は、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。AAA サーバの代わりにローカル データベースを使用して、ユーザ認証、許可、アカウンティングを提供することもがきます。詳細については、第 33 章「AAA のローカル データベースの設定」を参照してください。

AAA サービスのサポートの要約

表 32-1 は、特定の AAA サービス タイプのサポートを説明するコンフィギュレーション ガイドの章への相互参照を示します。

表 32-1　AAA サービスのサポート

AAA サービス	コンフィギュレーション ガイドの相互参照
証明書	第 40 章「デジタル証明書の設定」を参照してください。
アイデンティティ ファイアウォール	第 38 章「アイデンティティ ファイアウォールの設定」を参照してください。
Kerberos	VPN コンフィギュレーション ガイドの“Microsoft Kerberos Constrained Delegation Solution” section on page 78-61 を参照してください。
LDAP	第 36 章「LDAP サーバでの AAA の設定」を参照してください。
ローカル データベース	第 33 章「AAA のローカル データベースの設定」を参照してください。
NT	第 37 章「AAA 用 Windows NT サーバの設定」を参照してください。
RADIUS	第 34 章「AAA の RADIUS サーバの設定」を参照してください。
RSA/SDI	VPN コンフィギュレーション ガイドの、次の章を参照してください。 • Chapter 1, “Configuring IPsec and ISAKMP” • Chapter 3, “Setting General VPN Parameters” • Chapter 4, “Configuring Connection Profiles, Group Policies, and Users” • Chapter 6, “Configuring Remote Access IPsec VPNs,” • Chapter 8, “Configuring Easy VPN Services on the ASA 5505” • Chapter 10, “Configuring LAN-to-LAN IPsec VPNs”
TACACS+	第 35 章「AAA への TACACS+ サーバの設定」を参照してください。
TrustSec	第 39 章「Cisco TrustSec と統合するための ASA の設定」を参照してください。