概要

Cisco NX-OS ソフトウェアがサポートするセキュリティ機能を利用すると、パフォーマンスの劣化や障害からネットワークを保護できるだけでなく、故意に行われる攻撃や、善意のネットワーク ユーザの意図しない危険な間違いにより生ずるデータの紛失または毀損から保護することもできます。

- 認証、許可、アカウンティング，1 ページ
- RADIUS および TACACS+ セキュリティ プロトコル，2 ページ
- SSH および Telnet，3 ページ
- IP ACL，3 ページ

認証、許可、アカウンティング

Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）は、3 つの独立したセキュリティ機能をまとめて一貫性のあるモジュラ形式で設定するためのアーキテクチャ フレームワークです。

認証

ログイン/パスワードダイアログ、チャレンジ/レスポンス、メッセージング サポート、および暗号化（選択したセキュリティ プロトコルに基づく）などによるユーザの識別方法を提供します。 認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。 AAA 認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種インターフェイスに適用します。

許可

ワンタイム許可またはサービスごとの許可、ユーザ単位のアカウント リストとプロファイル、ユーザ グループ サポート、および IP、IPX、ARA、Telnet のサポートなど、リモートアクセスの制御方法を提供します。

RADIUS や TACACS+ などのリモート セキュリティ サーバでは、権限が定義された属性値（AV）のペアを、対象のユーザに関連付けることで、ユーザに対して特定の権限を許可します。 AAA 許可は、ユーザに許可されている操作を示す一連の属性を組み合わせて実行します。 これらの属性とデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制約事項が決定されます。

アカウンティング

ユーザ ID、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数といった、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信を行う手段を提供します。 アカウンティングを使用することで、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。

（注） 認証は AAA と別個に設定することができます。 ただし RADIUS または TACACS+ を使用する場合や、バックアップの認証方式を設定する場合は、AAA を設定する必要があります。

関連トピック

RADIUS および TACACS+ セキュリティ プロトコル

AAA は、セキュリティ機能の管理にセキュリティ プロトコルを使用します。 ルータまたはアクセス サーバがネットワーク アクセス サーバとして動作している場合は、ネットワーク アクセス サーバと RADIUS または TACACS+ セキュリティ サーバとの間の通信を確立する手段に、AAA が使用されます。

このマニュアルでは、次のセキュリティ サーバ プロトコルを設定する手順を説明します。

RADIUS

不正アクセスからネットワークを保護する分散型クライアント/サーバシステムです。RADIUS は AAA を使用して実装されます。 シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

TACACS+

ルータまたはネットワーク アクセス サーバにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。TACACS+ は AAA を使用して実装されます。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。 TACACS+ では、個別の、およびモジュールでの認証、許可、およびアカウンティング機能が提供されます。

関連トピック

SSH および Telnet

セキュア シェル（SSH）サーバを使用すると、SSH クライアントは Cisco NX-OS デバイスとの間でセキュアな暗号化された接続を確立できます。 SSH は強化暗号化を使用して認証を行います。 Cisco NX-OS ソフトウェアの SSH サーバは、市販の一般的な SSH クライアントと相互運用できます。

Cisco NX-OS ソフトウェアの SSH クライアントは、市販の一般的な SSH サーバと相互運用できます。

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。 Telnet を使用すると、あるサイトのユーザが別のサイトのログイン サーバと TCP 接続を確立し、キーストロークをデバイス間でやり取りできます。 Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

関連トピック

IP ACL

IP ACL は、トラフィックをパケットのレイヤ 3 ヘッダーの IPv4 情報に基づいてフィルタリングするために使用できるルールの順序セットです。 各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。 Cisco NX-OS ソフトウェアがパケットに IP ACL を適用するかどうか判定するときには、すべてのルールの条件に照らしてパケットを調べます。 最初の一致によってパケットを許可するか拒否するか判定します。一致するものがない場合は、Cisco NX-OS ソフトウェアは適切なデフォルト ルールを適用します。 Cisco NX-OS ソフトウェアは、許可されたパケットの処理を継続し、拒否されたパケットをドロップします。

関連トピック