TACACS+ と RADIUS の比較

内容

概要
前提条件
要件
使用するコンポーネント
表記法
RADIUS の背景情報
クライアント/サーバ モデル
ネットワーク セキュリティ
Flexible Authentication のメカニズム
サーバ コードの可用性
TACACS+ と RADIUS の比較
UDP と TCP
パケット暗号化
認証および認可
マルチプロトコル サポート
ルータ管理
相互運用性
トラフィック
デバイス サポート
関連情報

概要

ネットワークへのアクセスの制御に使用される 2 つの優れたセキュリティ プロトコルは Cisco TACACS+ と RADIUS です。RADIUS の仕様は、RFC 2865 に記述されています（これにより、RFC 2138 は廃止されました）。シスコはクラストップの製品によって、両方のプロトコルをサポートするために取り組んでいます。RADIUS と競合する、またはユーザが TACACS+ を使用するように影響を与えることは Cisco の意図するところではありません。お客様のニーズに合わせて最適なソリューションを選択してください。このドキュメントでは TACACS+ と RADIUS の違いについて説明し、理解した上で選択できるようにします。

Cisco は 1996 年 2 月の Cisco IOS® ソフトウェア リリース 11.1 以降、RADIUS プロトコルをサポートしています。Cisco は新しい機能と能力によって RADIUS クライアントの強化を続け、RADIUS を標準装備としてサポートしています。

Cisco は TACACS+ を開発する前に、セキュリティ プロトコルとしての RADIUS を真摯に評価しました。成長し続けるセキュリティ市場のニーズに合わせて、TACACS+ プロトコルには多くの機能が組み込まれています。このプロトコルはネットワークの規模の拡大に合わせて拡張し、市場の成熟に合わせて新しいセキュリティ技術を適用するために設計されました。TACACS+ プロトコルの基礎となるアーキテクチャは個別の認証、認可、およびアカウンティング（AAA）アー

キテクチャを補完します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメントの表記法の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

RADIUS の背景情報

RADIUS は、AAA プロトコルを使用するアクセス サーバです。ネットワークやネットワーク サービスのリモート アクセスを不正アクセスから保護する分散型セキュリティ システムです。RADIUS は、次の 3 つのコンポーネントで構成されています。

- ユーザ データグラム プロトコル（UDP）/IP を利用したフレーム形式のプロトコル
- サーバ 1 台
- クライアント 1 台

通常、サーバはカスタマーサイトの中央コンピュータで実行されます。クライアントはダイヤルアップ アクセス サーバにあり、ネットワーク中に分散が可能です。Cisco では、Cisco IOS ソフトウェア リリース 11.1 以降、およびその他のデバイス ソフトウェアに RADIUS クライアントを組み込んでいます。

クライアント/サーバ モデル

ネットワーク アクセス サーバ（NAS）は、RADIUS のクライアントとして動作します。クライアントは、ユーザ情報を目的の RADIUS サーバに渡し、返された応答に基づいて動作します。RADIUS サーバには、ユーザ接続要求を受け取り、ユーザを認証し、クライアントがユーザにサービスを提供するため必要なすべての設定情報を返す役割があります。RADIUS サーバは、他の種類の認証サーバに対しては、プロキシ クライアントとして動作します。

ネットワーク セキュリティ

クライアントと RADIUS サーバとの間のトランザクションは、共有秘密を使用して認証されます。共有秘密はネットワーク上に送信されることはありません。また、クライアントと RADIUS サーバ間では、すべてのパスワードが暗号化されて送信されます。これにより、保護されていないネットワーク上でユーザのパスワードがスヌーピングされ、特定されることがなくなります。

Flexible Authentication のメカニズム

RADIUS サーバは、ユーザを認証するさまざまな方法をサポートできます。ユーザが指定したユーザ名と元のパスワードを入力すれば、PPP、Password Authentication Protocol（PAP）または Challenge Handshake Authentication Protocol（CHAP）、Unix ログイン、およびその他の認証メカニズムをサポートできます。

サーバ コードの可用性

市販されている、および無料で使用できるサーバ コードは数多く流通しています。Cisco サーバには、Windows用 Cisco Secure ACS、Unix用 Cisco Secure ACS、および Cisco Access Registrar が含まれます。

TACACS+ と RADIUS の比較

次のセクションでは、TACACS+ と RADIUS のいくつかの機能を比較します。

UDP と TCP

RADIUS では UDP を使用し、TACACS+ では TCP を使用します。TCP は UDP に比べてさまざまなメリットがあります。TCP はコネクション型のトランスポートを提供する一方、UDP はベスト エフォート型の配信を提供します。RADIUS では、ベスト エフォート型のトランスポートを補正するため、再送信試行やタイムアウトなどの追加のプログラム可能な変数が必要ですが、TCP のトランスポートが提供するレベルの組み込み型のサポートは存在しません。

- TCP を使用すると、そのロード方法やバックエンド認証メカニズム（TCP 確認応答）がどの程度遅延しているかを問わず、（ほぼ）ネットワーク ラウンドトリップ時間（RTT）内で要求が受信されたという個別の確認応答を提供します。
- TCP はリセット（RST）によってサーバのクラッシュまたは動作停止状態を即時に示します。 長寿命の TCP 接続を使用すると、サーバがいつクラッシュし、サービスに復帰したかを判断することができます。UDP は、ダウンしたサーバ、低速のサーバ、および存在しないサーバを区別することはできません。
- TCP キープアライブを使用すると、サーバのクラッシュを、実際の要求によってアウトオブバンドで検出できます。複数のサーバへの接続を同時に保持することができ、動作中で実行中であることが判明しているサーバにのみ、メッセージを送信する必要があります。
- TCP はより拡張性が高く、成長を続ける、さらには輻輳されたネットワークにも対応します。

パケット暗号化

RADIUS では、クライアントからサーバへの Access-Request パケット内のパスワードしか暗号化されない。残りのパケットが暗号化解除される。このため、ユーザ名、正規サービス、アカウンティングなど、その他の他の情報が第三者にキャプチャされるおそれがある。

TACACS+ は、パケット本文は全体を暗号化するが、標準 TACACS+ ヘッダーは暗号化しない。ヘッダー内には、本文が暗号化されているかどうかを示すフィールドがあります。デバッグのためには、パケット本文を暗号化しない方が便利である。ただし、通常の動作では、通信のセキュア度を高めるためパケット本文は暗号化される。

認証および認可

RADIUS は認証と認可を結合する。RADIUS サーバからクライアントに送信される Access-Accept パケットには、認証情報が含まれます。このため、認証と認可を分けて考えることが困難です。

TACACS+ では、AAA を区別する AAA アーキテクチャを使用します。このため個別の認証ソリューションが実現し、認可とアカウンティング用には引き続き TACACS+ を使用することができます。たとえば、TACACS+ を使用すると、Kerberos の認証と TACACS+ の認可とアカウンティングを使用することができます。Kerberos サーバで NAS 認証を行うと、TACACS+ サーバから認証情報が要求され、再認証する必要はありません。NAS は TACACS+ サーバに Kerberos サーバ上で正常に認証されたことを通知し、サーバは認証情報を提供します。

セッションの間に追加の認証確認が必要になったら、アクセス サーバが TACACS+ サーバを使用して、特定のコマンドを使用する権限がユーザに付与されているかどうかを判別します。これにより、認証メカニズムから切り離しながら、アクセス サーバで実行可能なコマンドをより高度に制御できるようになります。

マルチプロトコル サポート

RADIUS は次のプロトコルをサポートしていません。

- AppleTalk Remote Access（ARA）プロトコル
- NetBIOS フレーム プロトコル制御プロトコル
- Novell Asynchronous Services Interface（NASI）
- X.25 PAD 接続

TACACS+ はマルチプロトコルをサポートしています。

ルータ管理

RADIUS では、ルータ上でどのコマンドを実行でき、どれを実行できないかをユーザが制御することはできません。したがって、RADIUS にはルータ管理の利便性や、ターミナル サービスのための柔軟性はありません。

TACACS+ には、ユーザ別またはグループ別にルータ コマンドの認可を制御する方法が 2 つあります。1 つ目の方法では、コマンドに特権レベルを割り当て、指定した特権レベルでユーザが認可されているかどうかについて、TACACS+ サーバを使用するルータで確認します。2 つ目の方法では、ユーザ別またはグループ別に、明示的に許可するコマンドを TACACS+ サーバに指定します。

相互運用性

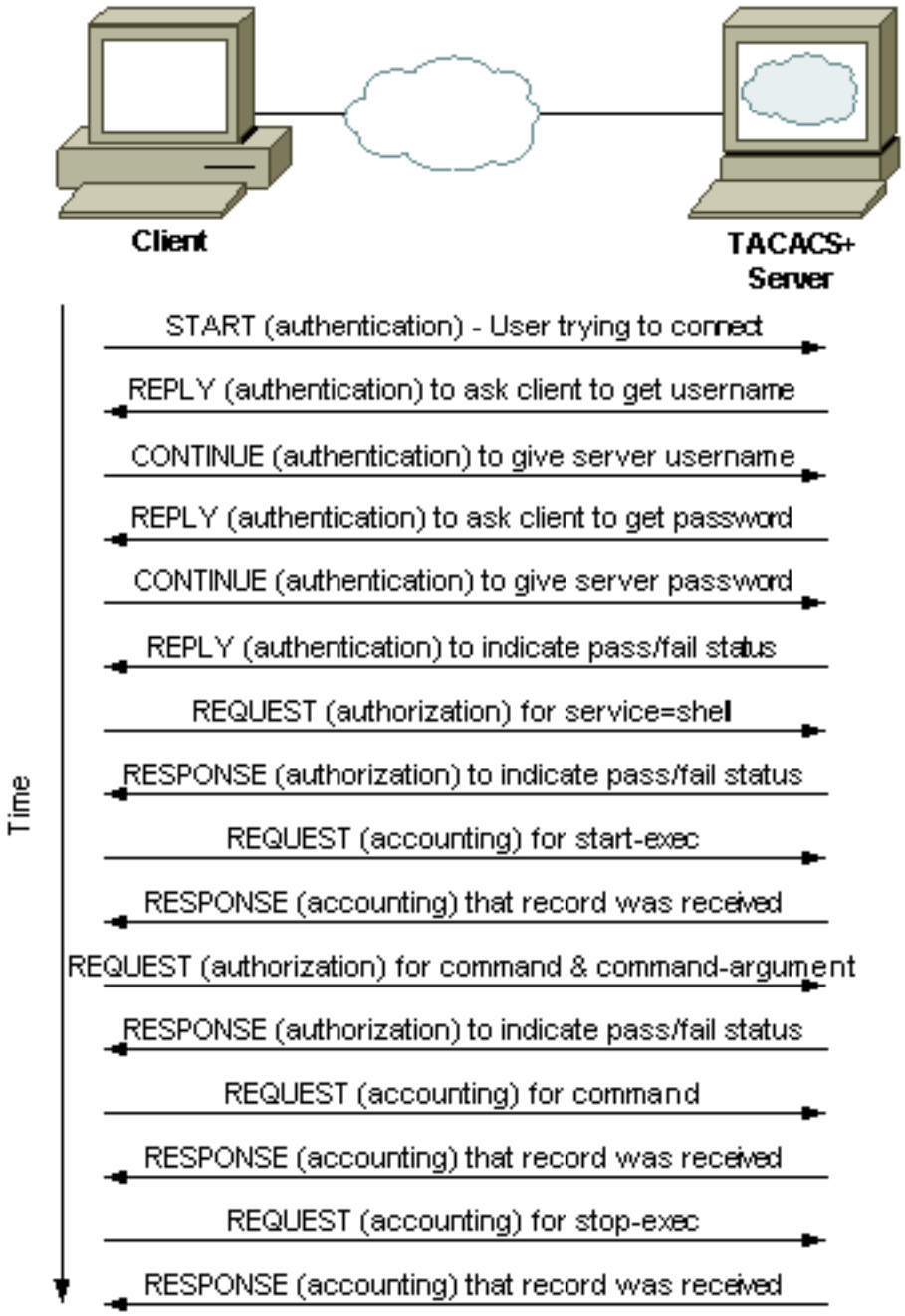
RADIUS Request For Comments（RFC）の解釈が多岐にわたるため、RADIUS RFC のコンプライアンスによって相互運用性が保証されるわけではありません。複数のベンダーが RADIUS クライアントを実装していますが、相互運用可能であることは意味しません。シスコではほとんどの RADIUS 属性を実装し、常に追加し続けています。お客様がそのサーバで標準の RADIUS 属性のみを使用する場合、複数のベンダーが同じ属性を実装する限り、そのベンダー間での相互運用が可能です。しかし、多くのベンダーが独自の属性である拡張機能を実装しています。お客様がこれらのベンダー固有属性のいずれかを使用している場合、相互運用はできません。

トラフィック

先ほど説明した TACACS+ と RADIUS の違いにより、クライアントとサーバの間で生成されるトラフィック量は異なります。次の例は、認証、EXEC 認可、コマンド認可（RADIUS では不可）、EXEC アカウンティングおよびコマンド アカウンティング（RADIUS では不可）を使用するルータ管理に使用されるときの、TACACS+ と RADIUS のクライアントとサーバ間のトラフィックを示しています。

TACACS+ のトラフィック例

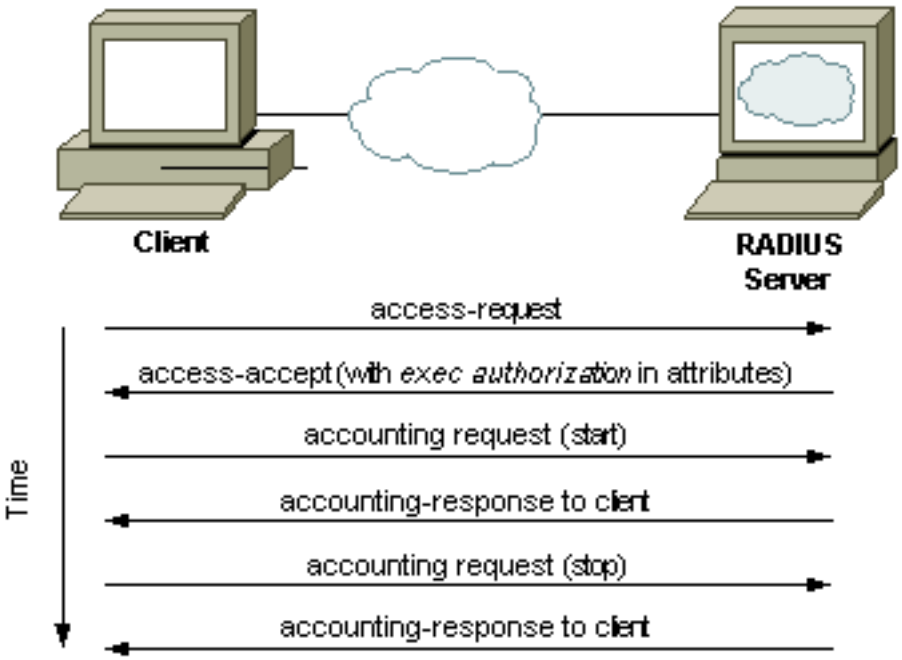
この例では、ユーザがルータに Telnets を行い、コマンドを実行し、ルータを終了するときに、ログイン認証、EXEC 認可、コマンド認可、開始/停止 EXEC アカウンティング、およびコマンド アカウンティングが TACACS+ に実装されてていると想定します。



RADIUS のトラフィック例

この例では、ユーザがルータに Telnets を行い、コマンドを実行し、ルータを終了するときに（他の管理サービスは利用不可）、ログイン認証、EXEC 認可、および開始/停止 EXEC アカウン

ティングが RADIUS に実装されていると想定します。



デバイス サポート

次の表は、選択したプラットフォームについて、デバイス タイプ別の TACACS+ と RADIUS AAA のサポートを示します。サポートが追加されたソフトウェア バージョンが含まれています。お使いの製品がこのリストになければ、製品の詳細について、リリース ノートを参照してください。

シスコ デバイス	TACACS+ 認証	TACACS+ 認可	TACACS+ アカウンティング	RADIUS 認証	RADIUS 認証	RADIUS アカウンティング
Cisco Aironet 1	12.2(4)JA	12.2(4)JA	12.2(4)JA	すべてのアクセス ポイント	すべてのアクセス ポイント	すべてのアクセス ポイント
Cisco IOS ソフトウェア [2]	10.33	10.33	10.33[3]	11.1.1	11.1.1[4]	11.1.1[5]
Cisco Cache Engine	—	—	—	1.5	1.5[6]	—
Cisco Catalyst スイッチ	2.2	5.4.1	5.4.1	5.1	5.4.1[4]	5.4.1[5]
Cisco CSS 11000	5.03	5.03	5.03	5.0	5.0[4]	—

Content Services Switch						
Cisco CSS 11500 Content Services Switch	5.20	5.20	5.20	5.20	5.20[4]	—
Cisco PIX ファイアウォール	4.0	4.0[7]	4.2[8,5]	4.0	5.2[7]	4.2[8,5]
Cisco Catalyst 1900/2820 スイッチ	8.x エンタープライズ[9]	—	—	—	—	—
Cisco Catalyst 2900XL/3500XL スイッチ	11.2.(8)SA6[10]	11.2.(8)SA6[10]	11.2.(8)SA6[10]	12.0(5)WC5[11]	12.0(5)WC5[11,4]	12.0(5)WC5[11,5]
Cisco VPN 3000 コンセントレータ[6]	3.0	3.0	—	2.0[12]	2.0	2.0[12]
Cisco VPN 5000 コンセントレータ	—	—	—	5.2X[12]	5.2X[12]	5.2X[12]

表の注記

1. ワイヤレス クライアントの終端のみ、Cisco IOS ソフトウェア リリース 12.2(4)JA 以降のバージョンの管理トラフィックは除く。Cisco IOS ソフトウェア リリース 12.2(4)JA 以降では、ワイヤレス クライアントおよび管理トラフィックの両方の終端で認証が行えます。
2. Cisco IOS ソフトウェア内のプラットフォーム サポートについては、Feature Navigator (後

継は Software Advisor（登録ユーザ専用））を確認します。
3. コマンド アカウンティングは、Cisco IOS ソフトウェア リリース 11.1.6.3 まで実装されません。
4. コマンド認可なし。
5. コマンド アカウンティングなし。
6. URL のブロックのみ、管理トラフィックなし。
7. PIX 経由の非 VPN トラフィックの認可。**注：リリース**5.2：アクセスコントロールリスト(ACL)のRADIUSベンダー固有属性(VSA)またはTACACS+許可をPIXリリース6.1で終端するVPNトラフィックのACL RADIUS属性11許可のサポート – ダウンロード可能ACLのサポートPIXリリース6.2で終端するVPNトラフィックに対してRADIUS認可を行う場合：TACACS+を介したPIX管理トラフィックに対する認可をサポートします。
8. PIX 経由の非 VPN トラフィックのアカウンティングのみ。管理トラフィックを除く。**注：リリース**5.2:PIXを介したVPN Client TCPパケットのアカウンティングのサポート。
9. エンタープライズ ソフトウェアのみ。
10. イメージには 8M のフラッシュが必要です。
11. VPN 終端のみ。

関連情報

- RADIUS に関するサポート ページ
- IOS での TACACS+ に関するドキュメント
- TACACS/TACACS+ サポート ページ
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems