セキュリティトラブルシューティングの概要

リモート アクセス

リモート アクセスを使用すると、必要なすべての装置に対して Terminal Services セッション（リモート ポート 3389）、HTTP セッション（リモート ポート 80）、および Telnet セッション（リモート ポート 23）を確立できます。

Caution ダイヤルインを設定する場合は、システムに対する脆弱性となるため、**login:cisco** または **password:cisco** は使用しないでください。

TACエンジニアが次のいずれかの方法を使用してデバイスにリモートアクセスすることを許可すると、多くの問題を非常に迅速に解決できます。

- パブリック IP アドレスが設定された装置
- ダイヤルインアクセス：（プリファレンスの高い順に）アナログモデム、統合デジタル通信網（ISDN）モデム、バーチャル プライベート ネットワーク（VPN）
- ネットワークアドレス変換（NAT）：プライベートIPアドレスが設定された装置へのアクセスを可能にする IOS およびプライベート インターネット エクスチェンジ（PIX）。

エンジニアの介入時にファイアウォールによって IOS トラフィックと PIX トラフィックが遮断されないこと、およびサーバ上で Terminal Services などの必要なすべてのサービスが開始されていることを確認してください。

Note TAC では、すべてのアクセス情報は厳重に管理されます。また、お客様の同意なしにシステムを変更することはありません。

Cisco Secure Telnet

Cisco Secure Telnet は、Cisco Service Engineers（CSE）がトランスペアレント ファイアウォールを使用してユーザのサイトにある Unified Communications Manager サーバにアクセスできる機能を提供します。

Cisco Secure Telnet は、シスコのファイアウォール内部で Telnet クライアントをイネーブル化することによって、ファイアウォールで稼働する Telnet デーモンに接続します。このセキュアな接続により、ファイアウォールの変更を行わずに Unified Communications Manager サーバをリモートモニタリングおよびメンテナンスできます。

Note シスコは、許可があった場合にだけお客様のネットワークにアクセスします。サイトに、このプロセスの開始を支援するネットワーク管理者を配置する必要があります。

ファイアウォールによる保護

ほとんどすべての内部ネットワークでは、外部から内部のホスト システムへのアクセスを制限するためにファイアウォール アプリケーションが使用されています。これらのアプリケーションでは、ネットワークとパブリック インターネットとの間のIP接続を制限することによって、ネットワークが保護されます。

ファイアウォールでは、許可するように明示的に再設定しないかぎり、外部から開始されるTCP/IP接続が自動的にブロックされます。

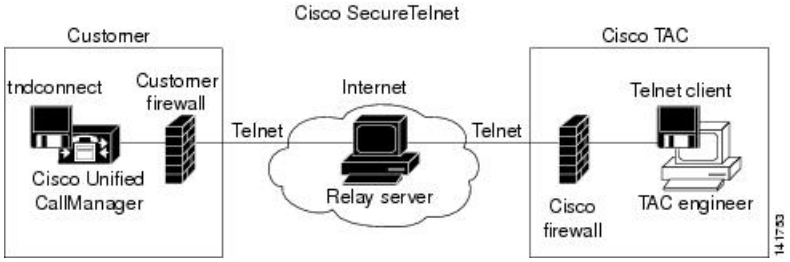
通常、企業ネットワークではパブリック インターネットとの通信が許可されますが、ファイアウォール内部から外部ホストに向けて開始される接続だけが許可されます。

Cisco Secure Telnet の設計

Cisco Secure Telnet では、ファイアウォールの内側から簡単に Telnet 接続を開始できるという技術を活用しています。外部のプロキシマシンを使用して、ファイアウォールの内側からのTCP/IP通信が *Cisco Technical Assistance Center*（TAC）にある別のファイアウォールの内側のホストへとリレーされます。

このリレー サーバを使用することによって、両方のファイアウォールの完全性が維持され、また保護されたリモート システム間の安全な通信がサポートされます。

***Figure 1: Cisco Secure Telnet* システム**



Cisco Secure Telnet の構造

外部のリレー サーバによって、お客様のネットワークとシスコとの間に Telnet トンネルが構築され、接続が確立されます。これにより、Unified Communications Manager サーバの IP アドレスとパスワード識別子を CSE に送信できます。

Note パスワードは、管理者と CSE が相互に同意した文字列です。

管理者は、Telnet トンネルを開始することによって、プロセスを開始します。これにより、ファイアウォールの内部からパブリック インターネット上のリレー サーバへの TCP 接続が確立されます。次に、Telnet トンネルによって、ローカルの Telnet サーバへの別の接続が確立され、エンティティ間の双方向のリンクが作成されます。

Note Cisco TAC の Telnet クライアントは、Windows NT および Windows 2000 上で動作するシステム、または UNIX オペレーティング システムに準拠して動作します。

ローカル サイトの Cisco Communications Manager がパスワードを受け入れると、Cisco TAC で実行されている Telnet クライアントは、ローカル ファイアウォールの内側で動作する Telnet デーモンに接続します。この結果確立される透過的接続によって、マシンがローカルで使用されている場合と同様にアクセスできるようになります。

Telnet 接続が安定した後、CSE はすべてのリモート有用性機能の機能を実装して、Unified Communications Manager サーバ上でメンテナンス、診断、およびトラブルシューティング タスクを実行できます。

CSE が送信するコマンド、および Unified Communications Manager サーバから発行される応答を表示することはできますが、コマンドや応答はすべてが完全な形式で表示されるわけではありません。

リモート アカウントの設定

シスコ サポートがトラブルシューティングのためにご使用のシステムに一時的にアクセスできるよう、Unified Communications Manager でリモート アカウントを設定します。

Procedure

Step 1 Cisco Unified Operating System Administration から、次を選択します。 **[サービス（Services）] > [リモートサポート（Remote Support）]**。

Step 2 [アカウント名（Account Name）] フィールドに、リモート アカウントの名前を入力します。

Step 3 [アカウントの有効期限（Account Duration）] フィールドに、アカウントの有効期限を日数で入力します。

Step 4 **[保存（Save）]** をクリックします。
システムは、暗号化パス フレーズを生成します。

Step 5 シスコのサポート担当者に連絡して、リモート サポート アカウント名とパス フレーズを提供します。