ネットワークセキュリティの保護とサードパーティへのアクセスの許可

内容

概要

このサービス要求の過程において、シスコ エンジニアを、貴社のネットワークへアクセスさせる場合があります。このようなアクセスを許可することにより、しばしば、サービス要求をより迅速に解決することができます。このような場合、シスコは、許可を得た場合に貴社のネットワークにアクセス可能であり、許可を得た場合しかアクセスを行いません。

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

ドキュメント表記の詳細は、『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。

ベスト プラクティス

Cisco では、所属している会社や組織外のサポート エンジニアなどにアクセスを許可する場合に、ネットワークのセキュリティを効果的に保護するためにこれらのガイドラインに従うことを推奨しています。

- 可能な場合は、サポート エンジニアと情報を共有するために、Cisco Unified MeetingPlace を使用してください。Cisco では、次の理由から Cisco Unified MeetingPlace の使用を推奨しています。Cisco Unified MeetingPlace は、一部のケースにおいてはセキュア シェル（SSH）や Telnet よりもさらに安全性の高い、セキュア ソケット レイヤ（SSL）プロトコルを使用します。Cisco Unified MeetingPlace は、会社や組織外の人にパスワードを提供する必要はありません。**注：社外または組織外のユーザにネットワークアクセスを許可する場合は、第三者がネットワークへのアクセスを要求する限り、ユーザが指定するパスワードは一時的なパスワードである必要があります。**ほとんどの企業向けファイアウォールがアウトバウンド HTTPS アクセスを許可しているため、Cisco Unified MeetingPlace がファイアウォール設定の変更を要求することは通常ありません。詳細については、『Cisco Unified MeetingPlace』をご覧ください。
- Cisco Unified MeetingPlace が使用できず、SSH のような他のアプリケーションを介したサード パーティ アクセスを許可することを選択した場合は、パスワードが一時的で 1 度のみしか使用できないことを確認してください。さらに、サード パーティ アクセスが不要になり次第、すぐにパスワードを変更するか無効にする必要があります。Cisco Unified MeetingPlace 以外のアプリケーションを使用する場合は、次の手順とガイドラインに従ってください。
  Cisco IOS ルータで一時的なアカウントを作成するには、次のコマンドを使用します。
  ```
  Router(config)#username tempaccount secret QWE!@#
  ```

  PIX/ASA で一時的なアカウントを作成するには、次のコマンドを使用します。
  ```
  PIX(config)#username tempaccount password QWE!@#
  ```

  一時的なアカウントを削除するには、次のコマンドを使用します。
  ```
  Router (config)#no username tempaccount
  ```

  一時パスワードをランダムに生成します。一時的なパスワードには、特定のサービス リクエストやサポート サービスのプロバイダーに関連しないものを使用する必要があります。たとえば、*cisco*、*cisco123*、または *ciscotac* などのパスワードは使用しないでください。あなた自身のユーザ名やパスワードは絶対に指定しないでください。インターネットを介して Telnet を使用しないでください。これは安全ではありません。
- サポートを必要とするシスコ デバイスが会社のファイアウォール外にあって、サポート エンジニアが SSH でシスコ デバイスに接続するためにファイアウォール ポリシーの変更が必要な場合、ポリシーの変更が、問題に割り当てられたサポート エンジニアに固有のものであることを確認します。決して、インターネット全体や必要以上のホストの広い範囲に、ポリシーの例外をオープンにすることのないようにしてください。Cisco IOS Firewall 上でファイアウォール ポリシーを変更するには、対インターネットのインターフェイスの下のインバウンド アクセスリストに、次の行を追加します。
  ```
  Router(config)#ip access-list ext inbound
  Router(config-ext-nacl)#1 permit tcp host
      <IP address for TAC engineer> host <Cisco device address> eq 22
  ```

  注：この例では、スペースを節約するため2Router(config-ext-nacl)#されています。ただし、インバウンド アクセスリストにこのコマンドを追加する場合は、構成は 1 行に表示する必要があります。Cisco PIX/ASA ファイアウォール上のファイアウォール ポリシーを変更するには、インバウンド アクセスグループに次の行を追加します。
  ```
  ASA(config)#access-list inbound line 1 permit tcp host
      <IP address for TAC engineer> host <Cisco device address> eq 22
  ```

  注：この例では、スペースを節約するたASA(config)#の設定が2行で表示されています。ただし、インバウンド アクセスグループにこのコマンドを追加する場合は、構成は 1 行に表示す

る必要があります。Cisco IOS ルータ上で SSH アクセスを許可するには、アクセスクラスに次の行を追加します。

```
Router(config)#access-list 2 permit host <IP address for TAC engineer>
Router(config)#line vty 0 4
Router(config-line)#access-class 2
```

Cisco PIX/ASA 上で SSH アクセスを許可するには、次の構成を追加します。

```
ASA(config)#ssh <IP address for TAC engineer> 255.255.255.255 outside
```

このドキュメントで説明されている情報に関して質問がある場合や追加の支援が必要な場合は、Cisco Technical Assistance Center (TAC) にお問い合わせください。

この Web ページは情報提供のみを目的としており、情報は「現状のまま」提供され、いかなる保証もありません。上記のベスト プラクティスは包括的ではありませんが、既存のセキュリティ プロセスを補完するために提示されます。すべてのセキュリティ対策の有効性は、個々のお客様の状況によって異なります。自社のネットワークに最適なセキュリティ プロセスを決定する際に、関連するすべての要因を考慮することが奨励されます。

関連情報

- Cisco Unified MeetingPlace
- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice (PIX を含む)
- Cisco Technical Assistance Center (TAC)
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems