IPSec の設定 - Cisco Secure VPN クライアントでのワイルドカード、事前共有キー、および No-mode Config

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[設定](#)
[ネットワーク図](#)
[設定](#)
[確認](#)
[トラブルシューティング](#)
[トラブルシューティングのためのコマンド](#)
[関連情報](#)

概要

この設定例では、ワイルドカード事前共有キー用に設定されたルータ（すべての PC クライアントが共通のキーを共有）を紹介します。 リモート ユーザはネットワークに入り、自身の IP アドレスを保持します。 リモート ユーザの PC とルータ間のデータは暗号化されます。

前提条件

要件

このドキュメントに関する固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情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® ソフトウェア リリース 12.2.8.T1
- Cisco Secure VPN Client バージョン 1.0 または 1.1：サポート終了
- DES イメージまたは 3DES イメージを保持する Cisco ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在

的な影響について確実に理解しておく必要があります。

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。

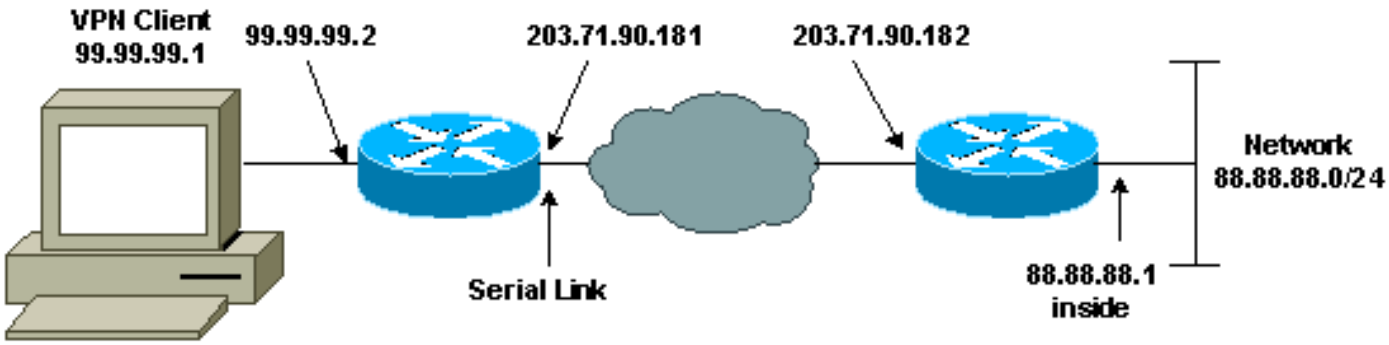
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは次の図に示すネットワーク



設定

このドキュメントでは次に示す設定を使用しています。

- ルータの設定
- VPN Client の設定

ルータの設定

```
Current configuration:
!
version 12.2

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RTCisco
!
enable password hjwwkj
!
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 203.71.57.242
!
```

```
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key mysecretkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test 10 ipsec-isakmp dynamic dyna
!
!
interface Serial0
ip address 203.71.90.182 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
crypto map test
!
interface Ethernet0
ip address 88.88.88.1 255.255.255.0
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.71.90.181
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password cscscs
login
!
end
```

VPN Client の設定

```
Current configuration:
!
version 12.2

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RTCisco
!
enable password hjwwkj
!
!
ip subnet-zero
ip domain-name cisco.com
ip name-server 203.71.57.242
!
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key mysecretkey address 0.0.0.0 0.0.0.0
!
```

```
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test 10 ipsec-isakmp dynamic dyna
!
!
interface Serial0
ip address 203.71.90.182 255.255.255.252
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
crypto map test
!
interface Ethernet0
ip address 88.88.88.1 255.255.255.0
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.71.90.181
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password cscscs
login
!
end
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show crypto isakmp sa**：フェーズ 1 のセキュリティ アソシエーションを表示します。
- **show crypto ipsec sa**：フェーズ 1 のセキュリティ アソシエーションとプロキシ、カプセル化、暗号化、カプセル化解除、および復号化情報を表示します。
- **show crypto engine connections active**：暗号化パケットと復号化パケットに関する現在の接続と情報を表示します。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

トラブルシューティングのためのコマンド

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされてい

ます。このツールを使用すると、**show** コマンド出力の分析を表示できます。

注: debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

注: 両方のピアでセキュリティ アソシエーションをクリアする必要があります。 非イネーブル モードで、ルータ コマンドを実行します。

注: 両方の IPSec ピアで次の debug コマンドを実行する必要があります。

- **debug crypto isakmp**：フェーズ 1 のエラーを表示します。
- **debug crypto ipsec**：フェーズ 2 のエラーを表示します。
- **debug crypto engine**：暗号化エンジンからの情報を表示します。
- **clear crypto isakmp**：フェーズ 1 のセキュリティ アソシエーションをクリアします。
- **clear crypto sa**：フェーズ 2 のセキュリティ アソシエーションをクリアします。

関連情報

- IPSec に関するサポート ページ
- VPN 3000 Client に関するサポートページ
- テクニカルサポート - Cisco Systems