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

内容

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しては個別の前提条件はありません。

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

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在

的な影響について理解しておく必要があります。

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。

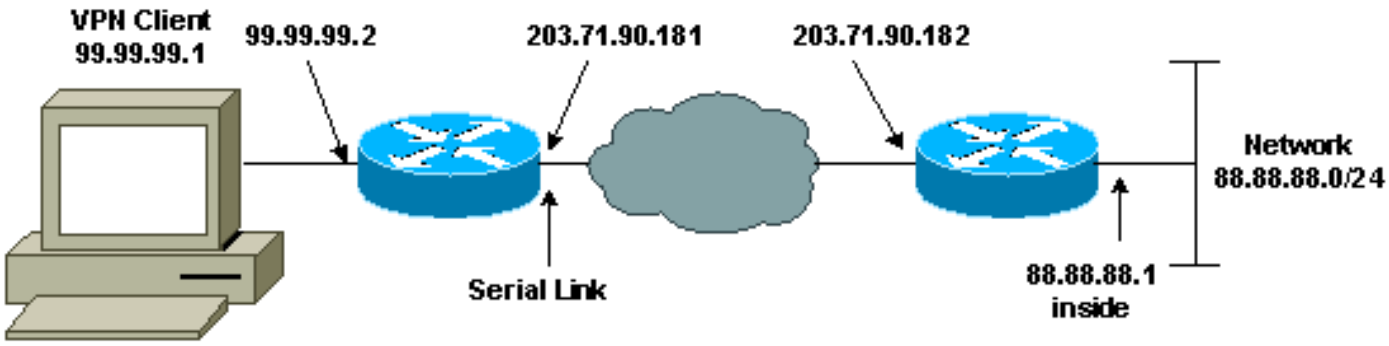
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください（登録ユーザのみ）。

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構成を使用しています。



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

```
Network Security policy:


1- Myconn
    My Identity
         Connection security: Secure
         Remote Party Identity and addressing
         ID Type: IP subnet
         88.88.88.0
         255.255.255.0
         Port all Protocol all


    Connect using secure tunnel
         ID Type: IP address
         203.71.90.182
```

```
    Authentication (Phase 1)
    Proposal 1

        Authentication method: Preshared key
        Encryp Alg: DES
        Hash Alg: MD5
        SA life:  Unspecified
        Key Group: DH 1

    Key exchange (Phase 2)
    Proposal 1
        Encapsulation ESP
        Encrypt Alg: DES
        Hash Alg: MD5
        Encap: tunnel
        SA life: Unspecified
        no AH

2- Other Connections
       Connection security: Non-secure
       Local Network Interface
         Name: Any
         IP Addr: Any
         Port: All
```

確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- **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。**

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

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

注：両方のピアの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：これらのデバッグは、両方のIPSecピアで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