

NAT を使用せずにルータのモードコンフィギュレーション、ワイルドカード事前共有キーを設定する方法

内容

[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](#)

[関連情報](#)

概要

この設定例では、ルータは、モード設定（プールから IP アドレスを取得）、ワイルドカード、事前共有キー（すべての PC のクライアントが共通のキーを共有）で、またネットワーク アドレス変換（NAT）なしに設定されています。オフサイト ユーザは、ネットワークを開始し、プールから内部 IP アドレスを割り当てられます。ユーザにとっては、ユーザがネットワーク内に見えるように見えます。ネットワーク内のデバイスは、ルーティング不可能な 10.2.1.x プールへのルートによって設定されます。

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いています。

- Cisco IOS®ソフトウェア12.0.7T以降
- このソフトウェアリビジョンをサポートするハードウェア
- CiscoSecure VPN Client 1.0/1.0.Aまたは1.1(それぞれ2.0.7/Eまたは2.1.12と表示され、[Help > About to check](#)に移動します)

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、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。

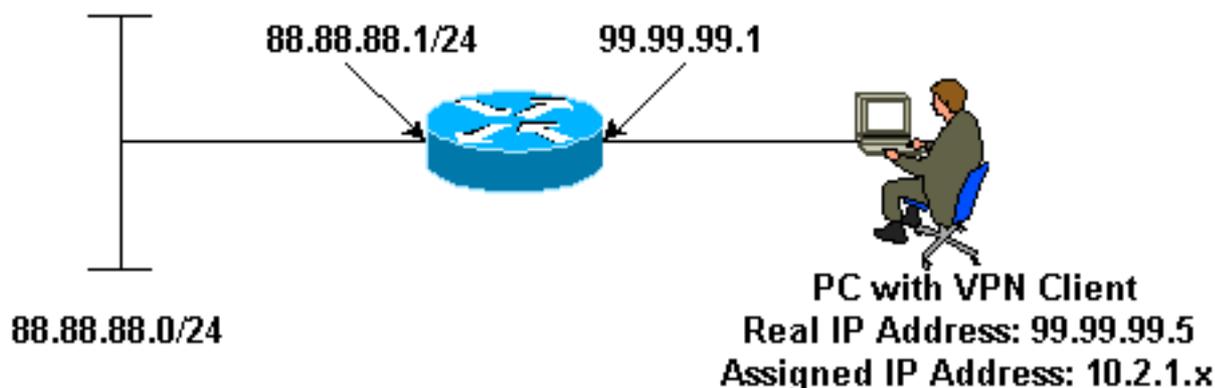
設定

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、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- VPN クライアント
- ルータ

```
VPN クライアント

Network Security policy:

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

    Connect using secure tunnel
```

```
ID Type: IP address
99.99.99.1
Pre-shared key = cisco123
```

Authentication (Phase 1)

Proposal 1

```
Authentication method: pre-shared 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
```

ルータ

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
enable password ww
!
username cisco password 0 cisco
!
clock timezone EST -5
ip subnet-zero
cns event-service server
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
crypto ipsec transform-set trans1 esp-des esp-md5-hmac
!
crypto dynamic-map dynmap 10
  set transform-set trans1
crypto map intmap client configuration address initiate
crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
!
```

```
interface Ethernet0

  ip address 99.99.99.1 255.255.255.0
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache

  crypto map intmap
!
interface Ethernet1
  ip address 88.88.88.1 255.255.255.0
  no ip directed-broadcast
!

ip local pool ourpool 10.2.1.1 10.2.1.254
ip classless
no ip http server
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
line vty 0 4
  password ww
  login
!
end
```

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 engine connections active - 暗号化パケットおよび復号化パケットを表示します。
- show crypto ipsec sa : フェーズ 2 のセキュリティ アソシエーションを表示します。
- 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。

これらのデバッグは、両方のIPSecルータ (ピア) で実行されている必要があります。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。

- debug crypto ipsec : フェーズ 2 の IPSec ネゴシエーションを表示します。
- debug crypto isakmp : フェーズ 1 の ISAKMP ネゴシエーションを表示します。
- debug crypto engine : 暗号化されたトラフィックを表示します。
- clear crypto isakmp : フェーズ 1 に関連したセキュリティ アソシエーションをクリアします。
- clear crypto sa : フェーズ 2 に関連したセキュリティ アソシエーションをクリアします。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [VPN 3000シリーズコンセントレータ製品に関するサポートページ](#)
- [Cisco VPN 3000 クライアント製品に関するサポート ページ](#)
- [IPSec\(IP Security Protocol\)テクノロジーに関するサポート](#)
- [テクニカルサポート - Cisco Systems](#)