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

目次

はじめに

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。 ユーザには、自分がネットワーク内にいるように見えます。 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関しては個別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 12.0.7T またはそれ以降
- 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 クライアント 1.0/1.0.A か 1.1（、それぞれ、チェックするために Help > About の順に進んで下さい 2.0.7/E か 2.1.12 として示されていて）

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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、次の設定を使用します。

- 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 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）で動作したにちがいありません。 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

現在のところ、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サポート
- Cisco VPN 3000 クライアント製品に関するサポート ページ
- IPSec（IPセキュリティプロトコル）技術サポート
- テクニカルサポート - Cisco Systems