配置路由器模式配置、萬用字元、預共用金鑰、無NAT

目錄

簡介

在此示例配置中，路由器配置為模式配置（從池獲取IP地址）、萬用字元預共用金鑰（所有PC客戶端共用一個公共金鑰），而不使用網路地址轉換(NAT)。 非現場使用者可以進入網路，並從池中分配內部IP地址。對於使用者而言，他們似乎位於網路內部。網路內的裝置設定路由到不可路由的10.2.1.x池。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS®軟體12.0.7T或更高版本
- 支援此軟體版本的硬體
- CiscoSecure VPN Client 1.0/1.0.A或1.1(分別顯示為2.0.7/E或2.1.12，請轉至**幫助>關於**以選中)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

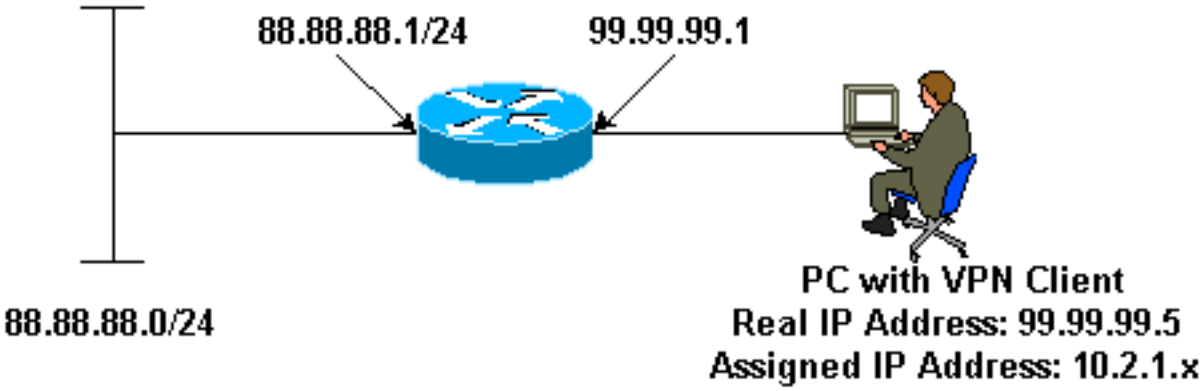
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- VPN使用者端
- 路由器

VPN使用者端

```
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
```

路由器

```
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
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

- **show crypto engine connections active** — 顯示加密和解密的資料包。
- **show crypto ipsec sa** — 顯示第2階段安全關聯。
- **show crypto isakmp sa** — 顯示第1階段安全關聯。

必須在兩台IPSec路由器（對等體）上運行這些調試。 必須在兩個對等體上清除安全關聯。

- **debug crypto ipsec** — 顯示第2階段的IPSec協商。
- **debug crypto isakmp** — 顯示第1階段的ISAKMP協商。
- **debug crypto engine** — 顯示加密的流量。
- **clear crypto isakmp** — 清除與第1階段相關的安全關聯。
- **clear crypto sa** — 清除與第2階段相關的安全關聯。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- VPN 3000系列集中器產品支援
- Cisco VPN 3000使用者端產品支援
- IPSec（IP安全通訊協定）技術支援
- 技術支援 - Cisco Systems