

# 配置路由器模式设置、通配符、预置共享密钥，不使用 NAT

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

在此示例配置中，针对模式配置（从池中获取 IP 地址）、通配符、预共享密钥（所有 PC 客户端共享一个密钥）配置路由器，而不进行网络地址转换 (NAT)。远端用户可以进入网络，并从池中获取一个内部 IP 地址。对于用户而言，他们看上去像位于网络内部。网络内的设备均设置为路由到不可路由的 10.2.1.x 池。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS 软件 12.0.7T 或以上
- 支持此软件修订版的硬件
- CiscoSecure VPN 客户端 1.0/1.0.A 或 1.1 (显示作为 2.0.7/E 或 2.1.12，分别，请去 [Help > About](#) 检查)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

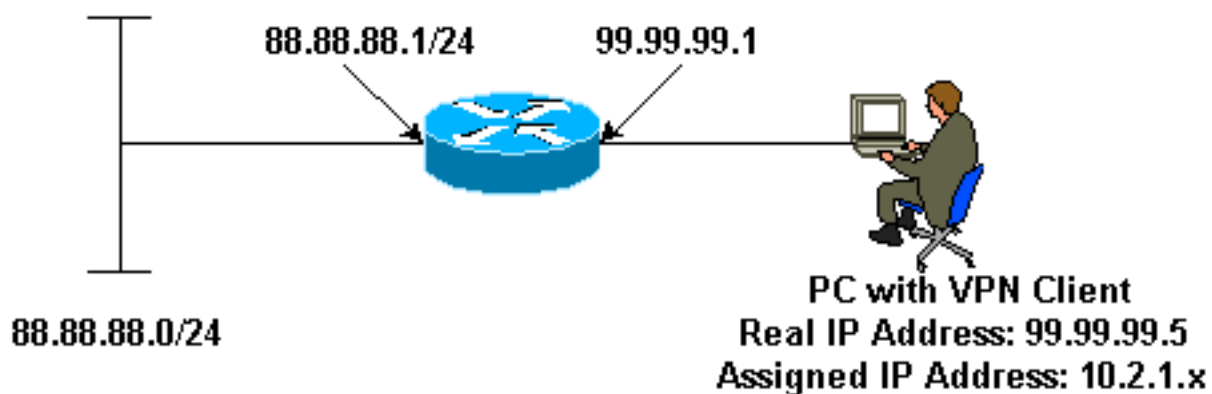
## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：**要查找本文档所用命令的其他信息，请使用 [命令查找工具](#)（仅限注册用户）。

## 网络图

本文档使用以下网络设置：



## 配置

本文档使用以下配置：

- VPN 客户
- 路由器

```
VPN 客户
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
```

## 验证

本部分所提供的信息可用于确认您的配置是否正常工作。

[命令输出解释程序工具](#) ( [仅限注册用户](#) ) 支持某些 **show** 命令，使用此工具可以查看对 **show** 命令输出的分析。

- **show crypto engine connections active** - 显示加密的数据包和解密的数据包。
- **show crypto ipsec sa** — 显示第 2 阶段安全连接。
- **show crypto isakmp sa** - 显示第 1 阶段的安全关联。

这些调试一定运行在两个IPSec路由器(对等体)。必须在两个对等体上清除安全关联。

- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** —显示阶段1的ISAKMP协商。
- **debug crypto engine** - 显示已加密的数据流。
- **clear crypto isakmp** - 清除与第 1 阶段相关的安全关联。
- **clear crypto sa** - 清除与第 2 阶段相关的安全关联。

## [故障排除](#)

目前没有针对此配置的故障排除信息。

## [相关信息](#)

- [VPN 3000系列集中器产品支持](#)
- [Cisco VPN 3000客户端产品支持](#)
- [IPSec \(IP安全协议\)技术支持](#)
- [技术支持 - Cisco Systems](#)