使用思科安全 VPN 客户端和无模式配置配置 IPSec - 通配符预共享密钥

目录

简介

此配置示例阐述了为通配符预共享密钥配置的路由器 - 所有 PC 客户端共享一个公用密钥。远程用户进入网络时保留自己的 IP 地址；远程用户的 PC 与路由器之间传输的数据经过加密。

先决条件

要求

本文档没有任何特定的前提条件。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- 思科 IOS® 软件 12.2.8.T1 版本
- 思科安全 VPN 客户端 1.0 或 1.1 版本 - 生命周期结束
- 带有 DES 或 3DES 镜像的思科路由器

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

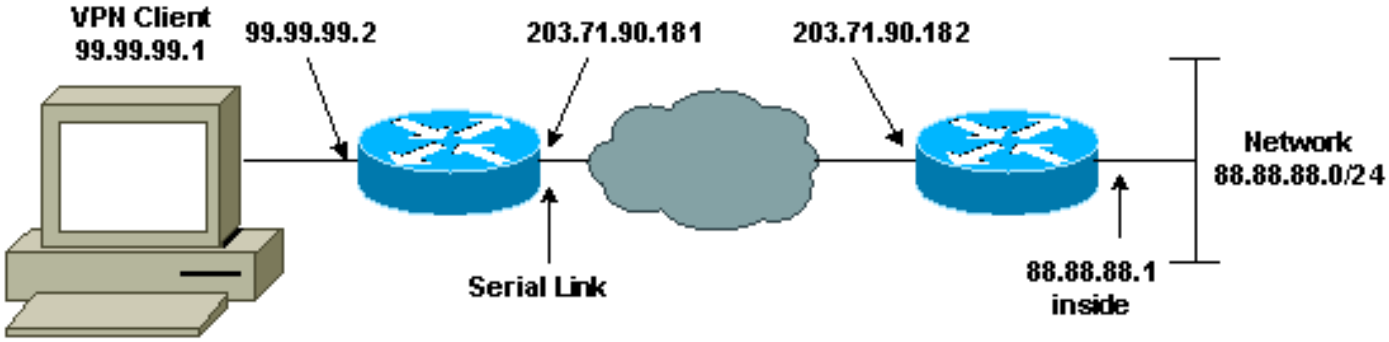
配置

本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用命令查找工具(仅注册客户)。

网络图

本文档使用下图所示的网络设置。



配置

本文档使用如下所示的配置。

- 路由器配置
- VPN 客户端配置

路由器配置

```
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 客户端配置

```
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
```

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 isakmp sa** - 显示第 1 阶段的安全连接。
- **show crypto ipsec sa - 显示阶段 1 的安全关联和代理、封装、加密、解封和解密信息。**
- **show crypto engine connections active - 显示当前连接及加密和解密数据包的相关信息。**

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

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。**

注意：在发出**debug**命令之前，请参阅有关Debug命令的重要信息。

注意：必须清除两个对等体上的安全关联。在非启用模式下执行路由器命令。

注意：必须在两个IPSec对等体上运行这些调试。

- **debug crypto isakmp** -显示在阶段1期间的错误。
- **debug crypto ipsec** -显示在阶段2期间的错误。
- **debug crypto engine - 显示来自加密引擎的信息。**
- **clear crypto isakmp - 清除第 1 阶段的安全连接。**
- **clear crypto sa - 清除第 2 阶段的安全连接。**

相关信息

- IPSec 支持页面
- VPN 3000 客户端支持页面
- 技术支持 - Cisco Systems