配置IPSec — 使用Cisco安全VPN客戶端和無模式配置來配置萬用字元預共用金鑰

目錄

簡介

此示例配置說明了為萬用字元預共用金鑰配置的路由器 — 所有PC客戶端共用一個公共金鑰。遠端使用者進入網路，保留自己的IP地址；遠端使用者的PC與路由器之間的資料會經過加密。

必要條件

需求

本文件沒有特定先決條件。

採用元件

本檔案中的資訊是根據以下軟體和硬體版本。

- Cisco IOS®軟體版本12.2.8.T1
- Cisco安全VPN客戶端1.0或1.1版 — 壽命終止
- 帶DES或3DES映象的Cisco路由器

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。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

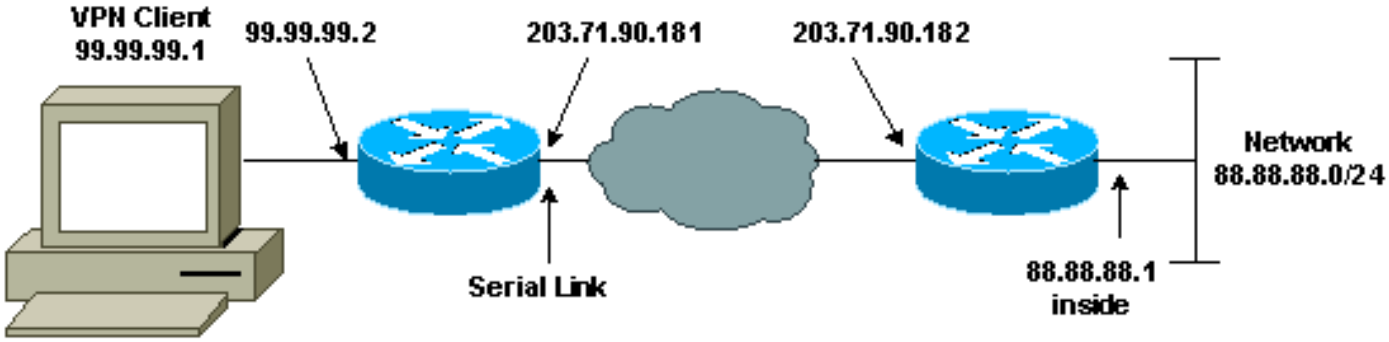
設定

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

本文檔使用下圖所示的網路設定。



組態

本文檔使用如下所示的配置。

- 路由器配置
- VPN客戶端配置

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客戶端配置

```
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
```

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 isakmp sa** — 顯示第1階段安全關聯。
- **show crypto ipsec sa** — 顯示第1階段安全關聯和代理、封裝、加密、解除封裝和解密資訊。
- **show crypto engine connections active** — 顯示當前連線以及有關加密和解密資料包的資訊。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

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。

注意：發出debug命令之前，請參閱有關Debug命令的重要資訊**。**

注意：您必須清除兩個對等體上的安全關聯。在非啟用模式下執行路由器命令。

注意：您必須在兩個IPSec對等體上運行這些調試。

- **debug crypto isakmp** — 顯示階段1期間的錯誤。
- **debug crypto ipsec** — 顯示階段2期間的錯誤。
- **debug crypto engine** — 顯示來自加密引擎的資訊。
- **clear crypto isakmp** — 清除第1階段安全關聯。
- **clear crypto sa** — 清除第2階段安全關聯。

相關資訊

- IPSec支援頁面
- VPN 3000客戶端支援頁

- 技術支援 - Cisco Systems