# 最初設定Cisco VPN 5000集中器並為遠端客戶端訪問

## 目錄



## 簡介

本指南介紹Cisco VPN 5000集中器的初始配置，尤其是如何將其配置為使用IP連線到網路，並提供遠端客戶端連線。

您可以根據將集中器連線到與防火牆相關的網路的位置，以兩種配置中的任一種來安裝集中器。集中器有兩個乙太網埠，其中一個埠(Ethernet 1)僅傳遞IPSec流量。另一個埠(Ethernet 0)路由所有IP流量。如果計畫與防火牆並行安裝VPN集中器，則必須使用兩個埠，以便乙太網0面向受保護的LAN，而乙太網1通過網路的網際網路網關路由器面向網際網路。您還可以將集中器安裝在受保護的LAN上的防火牆後面，並通過乙太網0埠將其連線，這樣Internet和集中器之間傳輸的IPSec流量就可以通過防火牆。

## 必要條件

### 需求

本文件沒有特定需求。

## 採用元件

本文檔中的資訊基於Cisco VPN 5000集中器。

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。

## 基本連線配置

建立基本網路連線的最簡單方法是將串列電纜連線到集中器上的控制檯埠，並使用終端軟體配置乙太網0埠上的IP地址。在乙太網0埠上配置IP地址後，可以使用Telnet連線到集中器以完成配置。您也可以在適當的文本編輯器中生成配置檔案，並使用TFTP將其傳送到集中器。

通過控制檯埠使用終端軟體時，系統最初會提示您輸入密碼。使用密碼「letmein」。 使用密碼響應後，發出**configure ip Ethernet 0**命令，以系統資訊響應提示。提示的順序應如下所示：

```
*[ IP Ethernet 0 ]# configure ip ethernet 0
      Section 'ip ethernet 0' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 0 ]# ipaddress=192.168.233.1
      *[ IP Ethernet 0 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 0 ]# ipbroadcast=192.168.233.255
      *[ IP Ethernet 0 ]# mode=routed
      *[ IP Ethernet 0 ]#
```

現在，您可以配置Ethernet 1埠。

### 乙太網1埠

Ethernet 1埠上的TCP/IP編址資訊是分配給集中器的可網際網路路由的外部TCP/IP地址。避免使用與Ethernet 0相同的TCP/IP網路中的地址，因為這將禁用VPN集中器中的TCP/IP。

輸入**configure ip ethernet 1**命令，以系統資訊響應提示。提示的順序應如下所示：

```
*[ IP Ethernet 0 ]# configure ip ethernet 1
      Section 'ip ethernet 1' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 1 ]# ipaddress=206.45.55.1
      *[ IP Ethernet 1 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 1 ]# ipbroadcast=206.45.55.255
      *[ IP Ethernet 1 ]# mode=routed
      *[ IP Ethernet 1 ]#
```

現在，您需要配置預設路由。

### 預設路由

您需要配置預設路由，集中器可以使用預設路由將所有TCP/IP流量傳送到與其直接連線的網路以外的網路或其具有動態路由的網路。預設路由指向在內部埠上找到的所有網路。稍後，您將使用IPSec Gateway引數配置Intraport以將IPSec流量傳送到Internet或從Internet傳送。要啟動預設路由配置，請輸入edit config ip static命令，以系統資訊響應提示。提示的順序應如下所示：

```
*IntraPort2+_A56CB700# edit config ip static
      Section 'ip static' not found in the config.
      Do you want to add it to the config? y
      Configuration lines in this section have the following format:
      <Destination> <Mask> <Gateway> <Metric> [<Redist=(RIP|none)>]
      Editing "[ IP Static ]"...
      1: [ IP Static ]
      End of buffer
      Edit [ IP Static ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> 0.0.0.0 0.0.0.0 192.168.233.2 1
      Append> .
      Edit [ IP Static ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

現在，您需要配置IPSec網關。

### IPSec閘道

IPSec網關控制集中器傳送所有IPSec流量或隧道流量的位置。這與您剛才配置的預設路由無關。首先輸入**configure general**命令，以系統資訊響應提示。提示的順序應如下所示：

```
* IntraPort2+_A56CB700#configure general
      Section 'general' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ General ]# ipsecgateway=206.45.55.2
      *[ General ]# exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

接下來，配置IKE策略。

## IKE策略

為集中器設定網際網路安全關聯金鑰管理協定/網際網路金鑰交換(ISAKMP/IKE)引數。這些設定控制集中器和客戶端如何識別和驗證彼此以建立隧道會話。此初始協商稱為階段1。階段1引數是裝置的全域性引數，不與特定介面相關聯。本節中識別的關鍵字說明如下。可在[Tunnel Partner <Section ID>]一節中設定LAN到LAN隧道的階段1協商引數。

第2階段IKE協商控制VPN集中器和客戶端如何處理各個隧道會話。在[VPN Group <Name>]裝置中設定VPN集中器和客戶端的第2階段IKE協商引數

IKE策略的語法如下：

```
Protection = [ MD5_DES_G1 | MD5_DES_G2 | SHA_DES_G1 | SHA_DES_G2 ]
```

protection關鍵字指定用於VPN集中器與客戶端之間的ISAKMP/IKE協商的保護套件。此關鍵字可在此部分內出現多次，在這種情況下，集中器將提議所有指定的保護套件。客戶端接受其中一個協商選項。每個選項的第一部分MD-5(message-digest 5)是用於協商的身份驗證演算法。SHA代表安全

雜湊演算法，它被認為比MD5更安全。每個選項的第二部分是加密演算法。DES（資料加密標準）使用56位金鑰對資料進行加擾。每個選項的第三個部分是Diffie-Hellman組，用於金鑰交換。由於組2(G2)演算法使用較大的數字，因此它比組1(G1)更安全。

要啟動配置，請輸入**configure IKE policy**命令，以系統資訊響應提示。

```
* IntraPort2+_A56CB700# configure IKE policy
      Section 'IKE Policy' was not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IKE Policy ] Protection = MD5_DES_G1
      *[ IKE Policy ] exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

配置基本資訊後，請輸入組引數。

# VPN組配置

輸入組引數時，請記住VPN組名稱不應包含空格，即使命令列解析器允許您在VPN組名稱中輸入空格。VPN組名稱可以包含字母、數字、短劃線和下劃線。

每個VPN組需要四個基本引數才能進行IP操作：

- Maxconnections
- StartIPaddress或LocalIPet
- 轉型
- IPNet

Maxconnections引數是此特定VPN組配置中允許的最大併發客戶端會話數。請記住此數字，因為它與StartIPAddress或LocalIPNet引數結合使用。

VPN集中器通過兩種不同的方案（StartIPAddress和LocalIPNet）將IP地址分配給遠端客戶端。StartIPAddress從連線到Ethernet 0的子網中分配IP號，並為連線的客戶端分配proxy-arp。LocalIPNet從VPN客戶端專有的子網中將IP號分配給遠端客戶端，並要求網路的其餘部分通過靜態或動態路由來瞭解VPN子網的存在。StartIPAddress提供更簡單的配置，但可能會限制地址空間的大小。LocalIPNet為遠端使用者提供了更大的定址靈活性，但需要稍稍增加一些工作來配置必要的路由。

對於StartIPAddress，請使用分配給傳入客戶端隧道會話的第一個IP地址。在基本配置設定中，這應該是內部TCP/IP網路（與乙太網0埠相同的網路）上的IP地址。 在下面的示例中，第一個客戶端會話分配了192.168.233.50地址，下一個併發客戶端會話分配了192.168.233.51等等。我們已經分配了Maxconnections值30，這意味著我們需要有一個30個未使用的IP地址塊(包括DHCP伺服器（如果有）)，其起始地址為192.168.233.50，終止地址為192.168.233.79。避免與不同VPN組配置中使用的IP地址重疊。

LocalIPNet將IP地址分配給來自LAN上其他位置必須未使用的子網的遠端客戶端。例如，如果您在VPN組配置中指定引數「LocalIPNet=182.168.1.0/24」，集中器會將IP地址分配給從192.168.1.1開始的客戶端。因此，您需要分配「Maxconnections=254」，因為集中器在使用LocalIPNet分配IP編號時不會注意子網邊界。

Transform關鍵字指定集中器用於IKE客戶端會話的保護型別和演算法。選項如下：

```
Transform = [ ESP(SHA,DES) | ESP(SHA,3DES) | ESP(MD5,DES) | ESP(MD5,3DES)
 | ESP(MD5) | ESP(SHA) | AH(MD5) | AH(SHA) |AH(MD5)+ESP(DES) | AH(MD5)+ESP(3DES)
 | AH(SHA)+ESP(DES) | AH(SHA)+ESP(3DES) ]
```

每個選項都是指定身份驗證和加密引數的保護部分。此關鍵字可在此部分內出現多次，在這種情況下，集中器將按照指定的保護片段的分析順序來建議它們，直到客戶端接受其中一個保護片段以供會話期間使用。大多數情況下，只需要一個Transform關鍵字。

ESP(SHA，DES)、ESP(SHA，3DES)、ESP(MD5,DES)和ESP(MD5,3DES)表示用於加密和驗證資料包的封裝安全負載(ESP)報頭。DES（資料加密標準）使用56位金鑰對資料進行加擾。3DES使用3個不同的金鑰和3個DES演算法的應用來加密資料。MD5是消息摘要5雜湊演算法，SHA是安全雜湊演算法，被認為比MD5更安全。

ESP(MD5,DES)是預設設定，建議用於大多數安裝。ESP(MD5)和ESP(SHA)使用ESP報頭驗證資料包，而不進行加密。AH(MD5)和AH(SHA)使用身份驗證報頭(AH)對資料包進行身份驗證。AH(MD5)+ESP(DES)、AH(MD5)+ESP(3DES)、AH(SHA)+ESP(DES)和AH(SHA)+ESP(3DES)使用身份驗證報頭對資料包進行身份驗證，ESP報頭對資料包進行加密。

**註：**Mac OS客戶端軟體不支援AH選項。如果使用Mac OS客戶端軟體，應至少指定一個ESP選項。

IPNet欄位非常重要，因為它控制著集中器客戶端可以前往的位置。在此欄位中輸入的值確定以隧道方式傳輸的TCP/IP流量，或者更常見的情況是，屬於此VPN組的客戶端可以進入您的網路。

思科建議設定內部網路(在本範例中為192.168.233.0/24)，因此所有從使用者端傳到內部網路的流量都會透過通道傳送，並進行驗證和加密（如果您啟用加密）。 在此案例中，沒有其他流量通過隧道傳輸；而是正常路由。可以有多個條目，包括單個或主機地址。格式是地址（在本例中是網路地址192.168.233.0），然後是與該地址關聯的掩碼（位為/24，即C類掩碼）。

輸入**configure VPN group basic-user**命令以開始此部分的配置，然後使用系統資訊對提示做出響應。以下是整個組態序列的範例：

```
*IntraPort2+_A56CB700# configure VPN group basic-user
      Section 'VPN Group basic-user' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ VPN Group "basic-user" ]# startipaddress=192.168.233.50
                                   or
      *[ VPN Group "basic-user" ]# localipnet=192.168.234.0/24
      *[ VPN Group "basic-user" ]# maxconnections=30
      *[ VPN Group "basic-user" ]# Transform=ESP(SHA,DES)
      *[ VPN Group "basic-user" ]# ipnet=192.168.233.0/24
      *[ VPN Group "basic-user" ]# exit
      Leaving section editor.
      *IntraPort2_A51EB700#
```

下一步是定義使用者的資料庫。

# VPN使用者配置

在配置的此部分中，定義VPN使用者資料庫。每行定義一個VPN使用者以及該使用者的VPN組配置和密碼。多行條目的換行符必須以反斜槓結尾。但是，用雙引號括起來的換行符將保留。

當VPN客戶端開始隧道會話時，客戶端的使用者名稱會傳輸到裝置。如果裝置在此部分找到使用者，則使用條目中的資訊設定隧道。（也可以使用RADIUS伺服器對VPN使用者進行身份驗證）。 如果裝置找不到使用者名稱，且您尚未設定RADIUS伺服器來執行驗證，則通道作業階段不會開啟，且錯誤會傳回使用者端。

輸入**edit config VPN users**命令開始配置。讓我們看一個將名為「User1」的使用者新增到VPN組「basic-user」的示例。

```
*IntraPort2+_A56CB700# edit config VPN users
      Section 'VPN users' not found in the config.
      Do you want to add it to the config? y
      <Name> <Config> <SharedKey>
      Editing "[ VPN Users ]"...
      1: [ VPN Users ]
      End of buffer
      Edit [ VPN Users ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> User1 Config="basic-user" SharedKey="Burnt"
      Append> .
      Edit [ VPN Users ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

此使用者的SharedKey為「Burnt」。 所有這些配置值都區分大小寫；如果配置「User1」，則使用者必須在客戶端軟體中輸入「User1」。輸入「user1」將導致無效或未經授權的使用者錯誤消息。您可以繼續輸入使用者，而不是退出編輯器，但是請記住，必須輸入一段時間才能退出編輯器。否則可能會導致組態中的專案無效。

# 結束

最後一步是儲存配置。當系統詢問您確定要下載配置並重新啟動裝置時，鍵入y並按Enter鍵。引導過程中不要關閉集中器。在集中器重新啟動後，使用者可以使用集中器VPN客戶端軟體進行連線。

要儲存配置，請輸入**save**命令，如下所示：

```
*IntraPort2+_A56CB700# save
      Save configuration to flash and restart device? y
```

如果使用Telnet連線到集中器，上面的輸出就是您看到的全部內容。如果通過控制檯連線，您只會看到類似以下內容的輸出，並且時間更長。在此輸出結束時，集中器返回「Hello控制檯……」 並要求輸入密碼。這就是你知道自己已經完成的方式。

```
Codesize => 0 pfree => 462
      Updating Config variables...
      Adding section '[ General ]' to config
      Adding -- ConfiguredFrom = Command Line, from Console
      Adding -- ConfiguredOn = Timeserver not configured
      Adding -- DeviceType = IntraPort2
      Adding -- SoftwareVersion = IntraPort2 V4.5
      Adding -- EthernetAddress = 00:00:a5:6c:b7:00
      Not starting command loop: restart in progress.
```

```
Rewriting Flash....
```

# 相關資訊

- Cisco VPN 5000系列集中器銷售終止公告
- Cisco VPN 5000集中器支援頁
- Cisco VPN 5000使用者端支援頁面
- IPsec支援頁面
- 技術支援與文件 - Cisco Systems