配置Cisco VPN 5000集中器並實施IPSec主模式LAN到LAN VPN連線

目錄

簡介

本文檔介紹Cisco VPN 5000集中器的初始配置，並演示如何使用IP連線到網路以及如何提供IPSec主模式LAN到LAN VPN連線。

您可以按照兩種配置中的任一種來安裝VPN集中器，具體取決於將其連線到與防火牆相關的網路的位置。VPN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VPN集中器安裝在受保護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流量便通過防火牆。

必要條件

需求

本文件沒有特定先決條件。

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。

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VPN集中器上的控制檯埠，然後使用終端軟體在乙太網0埠上配置IP地址。在乙太網0埠上配置IP地址後，可以使用Telnet連線到VPN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VPN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。提示序列應如下例所示。

```
*[ 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。

配置乙太網1埠

Ethernet 1埠上的TCP/IP編址資訊是您分配給VPN集中器的外部可網際網路路由的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。提示序列應如下例所示。

```
*[ 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IPSec網關。

配置IPSec網關

IPSec網關控制VPN集中器傳送所有IPSec流量或隧道流量的位置。這與稍後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。提示的順序應如下圖所示的示例所示。

```
* 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#
```

注意：在6.x及更高版本中，**ipsecgateway**命令已更改為**vpngateway命**令。

現在讓我們配置Internet金鑰交換(IKE)策略。

配置IKE策略

網際網路安全性關聯金鑰管理通訊協定(ISAKMP)/IKE引數控制VPN集中器和使用者端如何互相識別及驗證以建立通道作業階段。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VPN客戶端如何處理各個隧道會話。在[VPN組<名稱>]裝置中設定VPN集中器和VPN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集中器和VPN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，VPN集中器推薦所有指定的保護套件。VPN客戶端接受其中一個協商選項。每個選項的第一部分MD5（消息摘要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。示例如下。

```
* 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#
```

現在您已經配置了基本知識，現在應該定義隧道和IP通訊引數。

主模式站點到站點配置

要配置VPN集中器以支援LAN到LAN連線，您需要定義隧道配置以及要在隧道中使用的IP通訊引數。您將在兩個部分中執行此操作，[Tunnel Partner VPN x]部分和[IP VPN x]部分。對於任何給定的站點到站點配置，這兩個部分中定義的*x*必須匹配，以便隧道配置與協定配置正確關聯。

讓我們詳細瞭解其中的每個部分。

配置隧道合作夥伴部分

在隧道夥伴部分中，必須至少定義以下八個引數。

- 轉型
- 合作夥伴
- KeyManage
- SharedKey
- 模式
- 本地訪問
- 對等
- 繫結到

轉型

Transform關鍵字指定用於IKE客戶端會話的保護型別和演算法。與此引數關聯的每個選項都是指定身份驗證和加密引數的保護項。Transform引數可在此部分內出現多次，在這種情況下，VPN集中器會按照指定的保護片段的解析順序建議這些保護片，直到客戶端接受其中一個保護片以供會話期間使用。大多數情況下，只需要一個Transform關鍵字。

Transform關鍵字的選項如下。

```
[ 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) ]
```

ESP代表封裝安全負載，AH代表身份驗證報頭。這兩個標頭均用於加密和驗證封包。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，建議在大多數設定中使用。ESP(MD5)和ESP(SHA)使用ESP對資料包進行身份驗證（不加密）。AH(MD5)和AH(SHA)使用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AH對資料包進行身份驗證，ESP對資料包進行加密。

合作夥伴

Partner關鍵字定義隧道夥伴關係中其他隧道終結器的IP地址。此號碼必須是本地VPN集中器可以建立IPSec連線的公用、可路由IP地址。

KeyManage

KeyManage關鍵字定義隧道夥伴關係中的兩個VPN集中器如何確定發起隧道的裝置以及遵循何種隧道建立過程。選項包括自動、啟動、響應和手動。可以使用前三個選項配置IKE隧道，使用Manual關鍵字配置固定加密隧道。本文不介紹如何配置固定加密隧道。自動指定隧道夥伴可以啟動和響應隧道設定請求。Initiate指定隧道夥伴僅傳送隧道設定請求，而不響應它們。Respond指定隧道夥伴對隧道設定請求做出響應，但從不啟動它們。

SharedKey

SharedKey關鍵字用作IKE共用金鑰。您必須在兩個通道夥伴上設定相同的SharedKey值。

模式

Mode關鍵字定義IKE協商協定。預設設定為Aggressive，因此要將VPN集中器設定為互操作模式，必須將Mode關鍵字設定為Main。

本地訪問

LocalAccess定義可以通過隧道訪問的IP號，從主機掩碼到預設路由。LocalProto關鍵字定義可以通過隧道訪問哪些IP協定號，例如ICMP(1)、TCP(6)、UDP(17)等。如果要傳遞所有IP號，則應設定LocalProto=0。LocalPort確定可以通過隧道到達的埠號。LocalProto和LocalPort預設為0，或者全訪問。

對等

Peer關鍵字指定通過隧道找到的子網。PeerProto指定允許哪些協定通過遠端隧道端點，而PeerPort設定可在隧道另一端訪問的埠號。

繫結到

BindTo指定終止站點到站點連線的乙太網埠。應始終將此引數設定為Ethernet 1,VPN集中器以單埠模式運行時除外。

配置引數

要配置這些引數，請輸入**configure Tunnel Partner VPN 1**命令，以系統資訊響應提示。

提示序列應如下例所示。

```
*IntraPort2+_A56CB700# configure Tunnel Partner VPN 1
      Section ?config Tunnel Partner VPN 1? 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 "?"
      *[ Tunnel Partner VPN 1 ]# transform=ESP(MD5,DES)
      *[ Tunnel Partner VPN 1 ]# sharedkey=letmein
      *[ Tunnel Partner VPN 1 ]# partner=208.203.136.10
      *[ Tunnel Partner VPN 1 ]# mode=main
      *[ Tunnel Partner VPN 1 ]# peer=10.0.0.0/8
      *[ Tunnel Partner VPN 1 ]# localaccess=192.168.233.0/24
      *[ Tunnel Partner VPN 1 ]# bindto=Ethernet 1
      *[ Tunnel Partner VPN 1 ]# exit
      Leaving section editor.
```

現在應該配置IP部分。

配置IP部分

在每個隧道夥伴關係的IP配置部分中，您可以使用編號或未編號的連線（如在WAN連線上的IP配置中）。這裡，我們使用了未編號的。

未編號的站點到站點連線的最低配置需要兩個語句：numbered=false和mode=routed。首先輸入**configure ip vpn 1**命令，然後按照以下步驟響應系統提示。

```
*[ IP Ethernet 0 ]# configure ip vpn 1
      Section ?IP VPN 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 VPN 1 ]# mode=routed
      *[ IP VPN 1 ]# numbered=false
```

現在應該設定預設路由。

配置預設路由（TCP/IP路由表）

您需要配置預設路由，VPN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。您已使用IPSec網關引數配置了Intraport以將IPSec流量傳送到和從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。提示序列應如下例所示。

```
*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#
```

結束

最後一步是儲存組態。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**。引導過程中不要關閉VPN集中器。在集中器重新啟動後，使用者可以使用集中器的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
```

如果您使用Telnet連線到VPN集中器，上面的輸出就是您看到的全部內容。如果您通過控制檯連線，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，VPN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