初始设置 Cisco VPN 5000 集中器以及为远程客户端访问设置

目录

简介

本指南介绍Cisco VPN 5000集中器的初始配置，特别是如何配置它以使用IP连接到网络并提供远程客户端连接。

您可以按两种配置中的任意一种安装集中器，具体取决于您将集中器连接到与防火墙相关的网络的位置。集中器有两个以太网端口，其中一个（以太网1）只传递IPSec流量。另一个端口（以太网0）路由所有IP流量。如果计划与防火墙并行安装VPN集中器，则必须同时使用两个端口，使Ethernet 0面向受保护的LAN，而Ethernet 1通过网络的Internet网关路由器面向Internet。您还可以将集中器安装在受保护LAN的防火墙后，并通过Ethernet 0端口将其连接，以便Internet和集中器之间传输的IPSec流量通过防火墙。

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Cisco VPN 5000集中器。

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

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

基本连通性配置

建立基本网络连接的最简单方法是将串行电缆连接到集中器的控制台端口，并使用终端软件在Ethernet 0端口上配置IP地址。在Ethernet 0端口上配置IP地址后，您可以使用Telnet连接到集中器以完成配置。您还可以在适当的文本编辑器中生成配置文件，并使用TFTP将其发送到集中器。

通过控制台端口使用终端软件时，最初会提示您输入密码。使用密码“letmein”。 在用密码响应后，发出**configure ip Ethernet 0**命令，以响应系统信息提示。提示顺序应如下所示：

```
*[ 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 ]#
```

现在，您已准备好配置Ethernet 1端口。

Ethernet 1端口

Ethernet 1端口上的TCP/IP编址信息是您为集中器分配的外部、可路由的Internet TCP/IP地址。避免使用与Ethernet 0相同的TCP/IP网络中的地址，因为这将禁用VPN集中器中的TCP/IP。

输入configure ip ethernet 1**命令，以**响应系统信息提示。提示顺序应如下所示：

```
*[ 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 ]#
```

现在，您需要配置默认路由。

默认路由

您需要配置默认路由，集中器可以使用该路由将所有TCP/IP流量发送到与其直接连接或具有动态路由的网络以外的网络。默认路由指回内部端口上找到的所有网络。稍后，您将使用IPSec网关参数配置Intraport以向Internet发送IPSec流量，并从Internet发送IPSec流量。要启动默认路由配置，请输入edit config ip static命令，响应系统信息提示。提示顺序应如下所示：

```
*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#
```

现在，您需要配置IPSec网关。

IPSec 网关

IPSec网关控制集中器发送所有IPSec或隧道流量的位置。这与您刚配置的默认路由无关。首先输入**configure general**命令，用系统信息响应提示。提示顺序应如下所示：

```
* 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#
```

接下来，配置IKE策略。

IKE 策略

为集中器设置Internet安全关联密钥管理协议/Internet密钥交换(ISAKMP/IKE)参数。这些设置控制集中器和客户端如何相互识别和验证以建立隧道会话。此初始协商称为第1阶段。第1阶段参数对设备是全局的，不与特定接口关联。本节中识别的关键字如下所述。LAN到LAN隧道的第1阶段协商参数可在[Tunnel Partner <Section ID>]部分设置。

第2阶段IKE协商控制VPN集中器和客户端如何处理单个隧道会话。在[VPN组<Name>]设备中设置VPN集中器和客户端的第2阶段IKE协商参数

IKE策略的语法如下：

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

protection关键字指定VPN集中器和客户端之间ISAKMP/IKE协商的保护套件。此关键字可能在此部分中出现多次，在这种情况下，集中器建议所有指定的保护套件。客户端接受协商的选项之一。每个选项的第一个部分MD-5（消息摘要5）是用于协商的身份验证算法。SHA代表安全哈希算法，它

被认为比MD5更安全。每个选项的第二部分是加密算法。DES（数据加密标准）使用56位密钥对数据进行加扰。每个选项的第三部分是用于密钥交换的Diffie-Hellman组。由于组2 (G2)算法使用数更大，它比组1 (G1)更安全。

要启动配置，请输入**configure IKE policy**命令，以系统信息响应提示。

```
* 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#
```

配置了基础知识后，输入组参数。

VPN 组配置

输入组参数时，请记住，VPN组名称不应包含空格，即使命令行解析器允许您在VPN组名称中输入空格。VPN组名称可以包含字母、数字、破折号和下划线。

每个VPN组中需要四个基本参数来执行IP操作：

- 最大连接数
- StartIPaddress或LocalIPNet
- 转型
- IPNet

Maxconnections参数是此特定VPN组配置中允许的最大并发客户端会话数。请记住此数字，因为它与StartIPAddress或LocalIPNet参数配合使用。

VPN集中器通过两种不同方案（StartIPAddress和LocalIPNet）将IP地址分配给远程客户端。StartIPaddress为连接到Ethernet 0的子网分配IP编号，并为连接的客户端分配代理ARP。LocalIPNet从VPN客户端唯一的子网为远程客户端分配IP编号，并要求网络的其余部分通过静态或动态路由获知VPN子网的存在。StartIPaddress提供更简单的配置，但可能限制地址空间的大小。LocalIPNet为远程用户提供了更大的寻址灵活性，但配置必要的路由需要稍多一些工作。

对于StartIPAddress，使用分配给传入客户端隧道会话的第一个IP地址。在基本配置设置中，这应该是内部TCP/IP网络（与Ethernet 0端口相同的网络）上的IP地址。 在以下示例中，为第一个客户端会话分配了地址192.168.233.50，为下一个并发客户端会话分配了地址192.168.233.51，依此类推。我们分配了Maxconnections值30，这意味着我们需要有一个包含30个未使用IP地址的地址块（如果有，则包括DHCP服务器），从192.168.233.50开始，到192.168.233.79结束。避免与中使用的IP地址重叠不同的VPN组配置。

LocalIPNet从LAN中其他位置必须未使用的子网为远程客户端分配IP地址。例如，如果在VPN组配置中指定参数“LocalIPNet=182.168.1.0/24”，集中器将从192.168.1.1开始为客户端分配IP地址。因此，您需要分配“Maxconnections=254”，因为当使用Local分配IP编号时，集中器不会注意子网边界IPNet。

Transform关键字指定集中器用于IKE客户端会话的保护类型和算法。选项如下：

```
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) ]
```

每个选项都是一个保护条目，用于指定身份验证和加密参数。此关键字可能在此部分中出现多次，在这种情况下，集中器会按解析顺序提出指定的保护片段，直到客户端接受一个保护片段以供会话期间使用。在大多数情况下，只需一个Transform关键字。

ESP(SHA，DES)、ESP(SHA，3DES)、ESP(MD5,DES)和ESP(MD5,3DES)表示封装安全负载(ESP)报头，用于加密和验证数据包。DES（数据加密标准）使用56位密钥对数据进行加扰。3DES使用三种不同的密钥和三种DES算法的应用对数据进行加扰。MD5是消息摘要5哈希算法，SHA是安全哈希算法，被认为比MD5更加安全。

ESP(MD5,DES)是默认设置，建议用于大多数安装。ESP(MD5)和ESP(SHA)使用ESP报头对未加密的数据包进行身份验证。AH(MD5)和AH(SHA)使用身份验证报头(AH)对数据包进行身份验证。AH(MD5)+ESP(DES)、AH(MD5)+ESP(3DES)、AH(SHA)+ESP(DES)和AH(SHA)+ESP(3DES)使用身份验证报头对数据包进行身份验证，而ESP报头对数据包进行加密。

注意：Mac OS客户端软件不支持AH选项。如果使用Mac OS客户端软件，应至少指定一个ESP选项。

IPNet字段很重要，因为它控制集中器客户端可以到达的位置。在此字段中输入的值确定哪些TCP/IP流量是通过隧道传输的，或者更常见的是，属于此VPN组的客户端可以在您的网络中传输。

思科建议配置内部网络(本例中为192.168.233.0/24)，因此从客户端发往内部网络的所有流量都通过隧道发送，因此经过身份验证并加密（如果启用加密）。 在此场景中，没有其他流量通过隧道传输；而是正常路由。可以有多个条目，包括单个或主机地址。格式是地址（在本例中为网络地址192.168.233.0），然后是与该地址关联的掩码（位/24，即C类掩码）。

输入configure VPN group basic-user命令，**然后使用系统信息响应提示，以启动此部分配置。**以下是整个配置序列的示例：

```
*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#
```

下一步是定义用户的数据库。

VPN 用户配置

在配置的此部分，您定义VPN用户数据库。每行定义一个VPN用户以及该用户的VPN组配置和密码。多行条目必须以反斜杠结尾的换行符。但是，会保留双引号中的换行符。

当VPN客户端开始隧道会话时，客户端的用户名会传输到设备。如果设备在此部分中找到用户，则使用条目中的信息设置隧道。（您也可以使用RADIUS服务器对VPN用户进行身份验证）。 如果设备找不到用户名，并且您尚未配置RADIUS服务器以执行身份验证，则隧道会话不会打开，并且会向客户端返回错误。

输入edit config VPN users命**令启动配置**。让我们看一个将名为“User1”的用户添加到VPN组“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#
```

此用户的SharedKey为“已烧毁”。 所有这些配置值都区分大小写；如果配置“User1”，则用户必须在客户端软件中输入“User1”。输入“user1”会导致无效或未授权用户错误消息。您可以继续输入用户而不是退出编辑器，但请记住，必须输入句点才能退出编辑器。否则可能导致配置中的无效条目。

完成

最后一步是保存配置。当系统询问您是否确定要下载配置并重新启动设备时，键入y并按Enter键。在引导过程中请勿关闭集中器。集中器重新启动后，用户可以使用集中器VPN客户端软件进行连接。

要保存配置，请输入**save**命令，如下所示：

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

如果您使用Telnet连接到集中器，则上面的输出是您将看到的全部内容。如果通过控制台连接，您将看到类似以下的输出，只需更长时间。在此输出的末尾，集中器返回“Hello Console...” 并请求密码。你就是这么知道你完蛋的。

```
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....
```

相关信息

- Cisco VPN 5000 系列集中器终止销售公告
- Cisco VPN 5000 集中器支持页
- Cisco VPN 5000 客户端支持页
- IPSec 支持页面
- 技术支持和文档 - Cisco Systems