配置 Cisco VPN 5000 集中器，并实现 IPSec 主节点 LAN 到 LAN VPN 连通性

目录

简介

本文档介绍Cisco VPN 5000集中器的初始配置，并演示如何使用IP连接到网络以及如何提供IPSec主模式LAN到LAN VPN连接。

您可以按两种配置中的任意一种安装VPN集中器，具体取决于您将其连接到与防火墙相关的网络的位置。VPN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。您还可以在受保护LAN的防火墙后安装VPN集中器，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前提条件。

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VPN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VPN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VPN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。提示顺序应类似于以下示例。

```
*[ 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。

配置Ethernet 1 端口

Ethernet 1端口上的TCP/IP编址信息是您为VPN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。提示顺序应类似于以下示例。

```
*[ 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IPSec网关。

配置 IPSec 网关

IPSec网关控制VPN集中器发送所有IPSec或隧道流量的位置。这与您稍后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。提示的顺序应类似于下面所示的示例。

```
* 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：在版本6.x及更高版本中，**ipsecgateway**命令已更改为**vpngateway**命令。

现在，我们来配置Internet密钥交换(IKE)策略。

配置 IKE 策略

互联网安全关联密钥管理协议(ISAKMP)/IKE参数控制VPN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VPN客户端如何处理单个隧道会话。[VPN组<Name>]设备中设置了VPN集中器和VPN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关键字为VPN集中器和VPN客户端之间的ISAKMP/IKE协商指定保护套件。此关键字可能在此部分中出现多次，在这种情况下，VPN集中器建议所有指定的保护套件。VPN客户端接受协商的其中一个选项。每个选项的第一个部分MD5（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。示例如下所示。

```
* 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#
```

现在，您已配置了基础知识，是时候定义隧道和IP通信参数了。

主要模式站点到站点配置

要配置VPN集中器以支持LAN到LAN连接，您需要定义隧道配置以及要在隧道中使用的IP通信参数。您将在[Tunnel Partner VPN x]部分和[IP VPN x]部分两个部分完成此操作。对于任何给定的站点到站点配置，这两个部分中定义的*x*必须匹配，以便隧道配置与协议配置正确关联。

我们来详细了解一下每个部分。

配置Tunnel Partner部分

在隧道合作伙伴部分，必须至少定义以下八个参数。

- 转型
- 合作伙伴
- 密钥管理
- 共享密钥
- 模式
- LocalAccess
- 对等体
- 绑定到

转型

Transform关键字指定用于IKE客户端会话的保护类型和算法。与此参数关联的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。Transform参数可能在此部分中出现多次，在这种情况下，VPN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。

Transform关键字的选项如下。

```
[ 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代表封装安全负载，AH代表身份验证报头。这两个报头都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message-digest 5散列算法。SHA是安全散列算法，被认为比MD5更安全。

ESP(MD5,DES)是默认设置，建议用于大多数设置。ESP(MD5)和ESP(SHA)使用ESP对数据包进行身份验证（无加密）。AH(MD5)和AH(SHA)使用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AH验证数据包，ESP加密数据包。

合作伙伴

Partner关键字定义隧道伙伴关系中其他隧道终结器的IP地址。此编号必须是可路由的公有IP地址，本地VPN集中器可以使用该地址创建IPSec连接。

密钥管理

KeyManage关键字定义隧道伙伴关系中的两个VPN集中器如何确定启动隧道的设备以及要遵循的隧道建立过程类型。选项包括自动、启动、响应和手动。您可以使用前三个选项配置IKE隧道，使用Manual关键字配置固定加密隧道。本文档不介绍如何配置固定加密隧道。自动指定隧道合作伙伴可以发起和响应隧道设置请求。Initiate指定隧道合作伙伴仅发送隧道设置请求，而不响应这些请求。Respond指定隧道合作伙伴响应隧道设置请求，但从不发起请求。

共享密钥

SharedKey关键字用作IKE共享密钥。必须在两个隧道伙伴上设置相同的SharedKey值。

模式

Mode关键字定义IKE协商协议。默认设置为Aggressive，因此要将VPN集中器设置为互操作性模式，必须将Mode关键字设置为Main。

LocalAccess

LocalAccess定义可通过隧道访问的IP编号，从主机掩码到默认路由。LocalProto关键字定义哪些IP协议号可以通过隧道访问，例如ICMP(1)、TCP(6)、UDP(17)等。如果要传递所有IP编号，则应设置LocalProto=0。LocalPort确定哪些端口号可以通过隧道到达。LocalProto和LocalPort都默认为0或全访问。

对等体

Peer关键字指定通过隧道找到哪些子网。PeerProto指定允许哪些协议通过远程隧道终端，PeerPort设置哪些端口号可以在隧道的另一端访问。

绑定到

BindTo指定哪个以太网端口终止站点到站点连接。您应始终将此参数设置为Ethernet 1，除非VPN集中器在单端口模式下运行。

配置参数

要配置这些参数，请输入**configure Tunnel Partner VPN 1命令**，响应系统信息提示。

提示顺序应如下例所示。

```
*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.
```

现在是配置IP部分的时候了。

配置 IP 段

在每个隧道合作关系的IP配置部分，可以使用编号或未编号的连接（如WAN连接上的IP配置）。这里，我们用的是未编号的。

未编号的站点到站点连接的最低配置需要两条语句：numbered=false，mode=routed。首先输入**configure ip vpn 1**命令，然**后对系统提示做出如下响应。**

```
*[ 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
```

现在是时候设置默认路由了。

配置默认路由（TCP/IP 路由表）

您需要配置默认路由，VPN集中器可使用该路由将所有TCP/IP流量发往除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。您已使用IPSec网关参数将Intraport配置为向Internet发送IPSec流量，或从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#
```

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**。在引导过程中，请勿关闭VPN集中器。在集中器重新启动后，用户可以使用集中器的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VPN集中器，则上面的输出是您将看到的全部输出。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，VPN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