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

本文解释Cisco VPN 5000集中器的初始配置并且展示如何连接到网络使用IP和如何提供IPSec主模式LAN对LAN VPN连接。

您能安装在您连接它对网络关于防火墙两配置的之一的VPN集中器，根据。VPN集中器有两个以太网端口，其中之一(以太网1)仅通过IPSec数据流。另一个端口(Ethernet0)路由所有IP数据流。如果计划安装VPN集中器与防火墙平行，您必须使用两个端口，以便Ethernet0面对已保护LAN，并且Ethernet 1面对互联网到网络的互联网网关路由器。您能也安装在防火墙后的VPN集中器在已保护LAN和通过Ethernet0端口连接它，因此通过在互联网和集中器之间的IPSec数据流通过防火墙通过。

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

本文档中的信息根据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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

基本连通性配置

设立基本网络连接的简便的方法是连接串行电缆对VPN集中器的控制台端口和使用终端软件配置在Ethernet0端口的IP地址。在配置在Ethernet0端口的IP地址以后，您能使用Telnet连接到VPN集中器完成配置。使用TFTP，您能也生成在适当的文本编辑的一个配置文件，并且发送它到VPN集中器。

使用终端软件到控制台端口，最初提示对于密码。请使用密码“letmein”。在响应用密码以后，请发出**configure ip ethernet 0命令**，响应对与您的系统信息的提示符。提示符顺序应该看似类似以下示例。

```
*[ 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 ]#
```

现在您准备配置Ethernet 1端口。

配置Ethernet 1 端口

关于Ethernet 1端口的TCP/IP寻址信息是外部，您为VPN集中器分配的互联网可路由的TCP/IP地址。因为这将禁用在集中器的TCP/IP避免使用地址在TCP/IP网络和Ethernet0一样。

输入**配置ip Ethernet 1**命令，响应对与您的系统信息的提示符。提示符顺序应该看似类似以下示例。

```
*[ 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的地方或者建立隧道，流量。这您配置以后的对立于默认路由。开始通过输入**configure general命令**，响应对与您的系统信息的提示符。提示符顺序应该看似类似如下所示的示例。

```
* 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中和以后， **ipsecgateway命令**更改对**vpngateway命令**。

现在请配置Internet Key Exchange (IKE)策略。

配置 IKE 策略

互联网安全协会密钥管理协议(ISAKMP) /IKE参量控制VPN集中器和客户端如何识别并且互相验证建立隧道会话。相位1.阶段1参数是全局对设备和没有关联与特定接口，此初始协商被称为。在此部分认可的关键字下述。阶段1 LAN-to-LAN隧道的协商参数在[Tunnel Partner <Section ID>]部分可能设置。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。第2阶段VPN集中器和VPN客户端的IKE协商参数在[VPN Group <Name>]设备设置。

IKE策略的语法如下。

```
* 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#
```

Protection关键字指定ISAKMP/IKE协商的一个保护套件在VPN集中器和VPN客户端之间。在VPN集中器报价所有指定的保护套件情况下，此关键字可能多次出现在此部分内。VPN客户端接受其中一个协商的选项。每个选项第一部分， MD5 (消息摘要5)，是用于协商的验证算法。SHA代表安全散列算法，比MD5认为更多安全。每个选项第二部分是加密算法。DES (数据加密标准)使用一56位密钥加扰数据。每个选项第三部分是迪菲–赫尔曼组，用于密钥交换。由于组2 (G2)算法使用数更大，它比组1 (G1)更安全。

要开始配置，请输入**configure IKE policy命令**，响应对与您的系统信息的提示符。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#
```

即然您配置基础，是时间定义通道和IP通信参数。

主要模式站点到站点配置

要配置VPN集中器支持LAN-to-LAN连接，您需要定义隧道配置，以及用于通道的IP通信参数。您在两个部分、[Tunnel Partner VPN x]部分和[IP VPN x]部分将执行此。对于所有给的站点到站点配置，在这两个部分定义的*x*必须配比，因此隧道配置适当地关联与协议配置。

请详细查看这些部分中的每一个。

配置Tunnel Partner部分

在Tunnel Partner部分，您必须定义至少以下八个参数。

- 转换
- 合作伙伴
- KeyManage
- 共享键
- 模式
- LocalAccess
- 对等体
- BindTo

转换

Transform关键字指定用于IKE客户端会话和算法的保护类型。每个选项关联与此参数是指定验证和加密参数的保护部分。转换参数可能多次出现在此部分内，在VPN集中器报价指定的保护部分按在会话期间，他们解析的顺序情况下，直到一个人由客户端接受为使用。在大多数情况下，仅一Transform关键字是需要的。

Transform关键字的选项如下。

```
* 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#
```

ESP代表封装安全有效载荷，并且AH代表认证报头。这两个报头用于加密和验证数据包。DES (数据加密标准)使用一56位密钥加扰数据。3DES使用三不同的密钥和DES算法的三应用程序加扰数据。MD5是message-digest 5散列算法。SHA是安全散列算法，比MD5认为稍微更多安全。

ESP(MD5,DES)是默认设置和为多数设置推荐。ESP(MD5)和ESP(SHA)使用ESP验证数据包(没有加密)。AH(MD5)和AH(SHA)使用AH验证数据包。AH(MD5)+ESP(DES)、AH(MD5)+ESP(3DES)、

AH(SHA)+ESP(DES)和AH(SHA)+ESP(3DES)使用AH验证数据包和ESP加密数据包。

合作伙伴

对端关键字定义了另一个隧道终止器的IP地址在通道合伙企业的。此编号必须是公共，本地VPN集中器能创建IPSec连接的可路由IP地址。

KeyManage

KeyManage关键字定义了在通道合伙企业的两个VPN集中器如何确定跟随的哪个设备发起通道，并且什么类型的隧道建立过程。选项是Auto， Initiate， Respond及Manual。您能使用三第一选择配置IKE通道和Manual关键字配置固定加密隧道。本文不包括如何配置固定加密隧道。自动指定隧道贸易伙伴能启动和回答隧道设置请求。启动指定隧道贸易伙伴只发送隧道设置请求，它不响应对他们。请勿响应指定隧道贸易伙伴回答隧道设置请求，但是启动他们。

共享键

共享密钥关键字使用作为IKE共享的机密。您必须设置在两个隧道贸易伙伴的同一个SharedKey值。

模式

模式关键字定义了IKE协商协议。默认设置是积极的，因此设置互操作性模式的VPN集中器，您必须设置模式关键字为主。

LocalAccess

LocalAccess定义了可以通过通道访问的IP编号，从主机掩码到默认路由。IP协议编号可以通过通道访问，例如ICMP(1)， TCP(6)， UDP(17)，等等的LocalProto关键字定义了。如果要通过所有IP编号，则您应该设置LocalProto=0。LocalPort确定哪些端口号可以通过通道到达。LocalProto和LocalPort默认为0或者所有访问。

对等体

对等体关键字指定哪些子网通过通道被找到。PeerProto指定哪些协议通过远程隧道终点允许和端口号可以访问在通道的另一端的PeerPort集。

BindTo

BindTo指定哪个以太网端口终止站点到站点连接。当VPN集中器在单端口模式时，运行您应该总是设置此参数为Ethernet 1，除了。

配置参数

要配置这些参数，请输入**configure Tunnel Partner VPN 1命令**，响应对与您的系统信息的提示符。

提示符顺序应该看似类似下面示例。

```
*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.
```

现在是时间配置IP段。

配置 IP 段

您在每家通道合伙企业的IP配置部分能使用编号或未编号的连接(正如在广域网连接的IP配置)。这里，我们使用了未编号的。

未编号的站点到站点连接的最低配置要求两个语句：numbered=false和mode=routed。开始通过输入**配置ip VPN 1**命令，和响应对系统提示符如下。

```
*[ 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
```

现在是时间设置默认路由。

配置默认路由（TCP/IP 路由表）

您需要配置VPN集中器能使用发送为网络注定的所有TCP/IP流量除网络之外直接地连接，或者为的默认路由哪些把动态路由。回到在内部端口找到的所有网络的默认路由点。使用IPSec网关参数，您已经配置Intraport到/从互联网发送IPSec数据流。要开始默认路由配置，请输入edit config ip static命令，响应对与您的系统信息的提示符。提示符顺序应该看似类似下面示例。

```
*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。当询问，如果肯定您要下载配置和重新启动设备，键入**y**并且按回车。请勿在启动程序中关闭VPN集中器。在集中器重新启动后，使用集中器的VPN客户端软件，用户能连接。

要保存配置，请输入**save命令**，如下。

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

使用Telnet，如果连接到VPN集中器，以上输出是您将看到的所有。如果通过控制台连接，您将看到输出类似于以下，只更加长。在此输出结束时， VPN集中器返回“Hello控制台…”并且请求密码。这是您如何知道您完成。

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

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