目录

简介

使用IP，此指南解释Cisco VPN 5000集中器的初始配置，特别地如何配置它连接到网络，并且提供远程客户端连接。

您能安装在您连接它对网络关于防火墙两配置的之一的集中器，根据。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要求。

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 ]#
```

现在您准备配置Ethernet 1端口。

Ethernet 1端口

关于Ethernet 1端口的TCP/IP寻址信息是外部，您为集中器分配的互联网可路由的TCP/IP地址。因为这将禁用在VPN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，以后，您将配置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的地方或者建立隧道，流量。这您配置的对立于默认路由。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#
```

其次，请配置IKE策略。

IKE 策略

设置集中器的互联网安全协会密钥管理协议/互联网密钥交换(ISAKMP/IKE)参数。这些设置控制集中器和客户端如何识别并且互相验证为了建立隧道会话。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协商控制如何VPN集中器和客户端处理各自的隧道会话。第2阶段VPN集中器和客户端的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集中器和客户端之间。在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。客户端接受其中一个协商的选项。每个选项第一部分， MD-5 (message-digest 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。

```
* 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#
```

即然基础配置，请输入组参数。

VPN 组配置

当输入组参数时，请记住VPN组名称不应该包含空间，即使命令行分析程序允许您输入在VPN组名称的空间。VPN组名称能包含字母、编号、破折号和下划线。

有在IP操作的每个VPN组中要求的四个基本参数：

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

最大连接数参数是在此特定的VPN组配置方面允许的并发客户端会话最大。记住此编号，与

StartIPaddress或LocalIPNet参数一道工作。

VPN集中器分配IP地址到远程客户端由两不同机制、StartIPaddress和LocalIPNet。StartIPaddress分配从连接的子网的IP编号到Ethernet0和proxy-arps为连接的客户端。LocalIPNet分配IP编号到从子网的远程客户端唯一对VPN客户端，并且要求网络的其余意识到VPN子网的存在通过静态或动态路由。StartIPaddress提供更加容易的配置，但是可能限制地址空间的大小。LocalIPNet提供编址的较大适应性远程用户的，但是要求轻微更多工作配置必要路由。

对于StartIPaddress，请使用第一个IP地址分配到一流入客户端隧道会话。在基本配置配置设置，这应该是在内部TCP/IP网络(网络的一个IP地址和Ethernet0端口一样)。在下面的示例中我们的，第一客户端会话分配192.168.233.50地址，下并发客户端会话分配192.168.233.51，等等。我们分配最大连接数值为30，含义需要有30个未使用IP地址块(包括DHCP服务器，如果有其中任一)开始与192.168.233.50和结束以192.168.233.79的我们。避免交迭用于不同的VPN组配置的IP地址。

LocalIPNet分配IP地址到从一定在别处是未使用在LAN的子网的远程客户端。例如，如果在VPN组配置里指定参数"LocalIPNet=182.168.1.0/24"，集中器分配IP地址到开始与192.168.1.1的客户端。所以，您需要分配"Maxconnections=254"，因为集中器不会注意子网限定范围，当分配IP编号使用LocalIPNet时。

Transform关键字指定集中器使用IKE客户端会话的保护类型和算法。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#
```

每个选项是指定验证和加密参数的保护部分。此关键字可能多次出现在此部分内，在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。

ESP (SHA， DES)， ESP(SHA,3DES)、ESP(MD5,DES)和ESP(MD5,3DES)表示封装安全有效载荷(ESP)报头加密和验证数据包。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，并且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安装推荐。ESP(MD5)和ESP(SHA)使用ESP报头验证数据包没有加密。AH(MD5)和AH(SHA)使用认证报头(AH)验证数据包。AH(MD5)+ESP(DES)、AH(MD5)+ESP(3DES)、AH(SHA)+ESP(DES)和AH(SHA)+ESP(3DES)使用认证报头验证数据包和ESP报头加密数据包。

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，您应该指定至少一个ESP选项。

IPNet字段是重要，因为控制集中器客户端可以去的地方。您在此字段输入的值确定什么TCP/IP流量被建立隧道，或者通常，其中属于此VPN组的客户端在您的网络可以去。

思科推荐配置内部网络(在本例中192.168.233.0/24)，因此从去内部网络的客户端的所有流量通过通道发送，并且验证并且加密(如果启用加密)。在此方案中，其他流量没有被以隧道传输;反而，它通常路由。您能有多个条目，包括单个或主机地址。格式是地址(在我们的示例，网络地址192.168.233.0)然后掩码关联与该地址在位(/24，是C类掩码)。

通过输入**configure VPN group basic-user命令**开始配置的这部分，然后响应对与您的系统信息的提示符。这是整个配置顺序的示例：

```
*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#
```

下一步是定义用户数据库。

VPN 用户配置

在配置的此部分，您定义了VPN用户数据库。每条线路与该用户的VPN组配置和密码一起定义了VPN用户。多线条目必须有结束以斜线的线路中断。然而，在放入的线路中断双引号保留。

当VPN客户端开始隧道会话时，客户端的用户名传送到设备。如果设备寻找此部分的用户，在条目使用信息设置通道。(您能也使用RADIUS服务器VPN用户的验证)。如果设备没找到用户名，并且未配置RADIUS服务器执行验证，没有召开隧道会话，并且错误返回给客户端。

通过输入**edit config VPN users命令**开始配置。请查看添加一个用户名为"User1"到VPN组“基本用户”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#
```

此用户的共享键“烧录”。所有这些配置值区分大小写;如果配置"User1"，用户必须输入"User1"在客户端软件里。输入"user1"导致一无效或未经授权的用户错误消息。您能继续输入用户而不是退出编辑器，但是记住，您必须输入期限退出编辑器。失败能在配置里导致无效条目。

完成

您的最后一步保存配置。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Enter键。请勿在启动程序中关闭集中器。在集中器重新启动后，使用集中器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，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