配置 Cisco VPN 3000 集中器到 Cisco 路由器的连接

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[网络图](#)
[配置](#)
[VPN 集中器配置](#)
[验证](#)
[在路由器上](#)
[在 VPN 集中器上](#)
[故障排除](#)
[在路由器上](#)
[问题-无法发起通道](#)
[PFS](#)
[相关信息](#)

简介

此配置示例显示如何连接一私有网络在运行Cisco IOS软件到私有网络在Cisco VPN 3000集中器后的路由器背后。网络上的设备通过专用地址互相通信。

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以下软件和硬件版本：

- 有Cisco IOS软件版本12.3.(1)a的Cisco 2611路由器**注意：** 确保Cisco 2600系列路由器安装与支持VPN功能的一个crypto IPSec VPN IOS镜像。
- 有4.0.1的B Cisco VPN 3000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。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用此网络设置。

配置

本文档使用以下配置。

路由器配置

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
```

```
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

VPN 集中器配置

在此实验室设置， VPN集中器通过控制台端口首先访问，并且最小配置被添加，以便进一步配置可以通过图形用户界面(GUI)被执行。

选择**Administration > System Reboot > Schedule reboot > Reboot with Factory/Default Configuration**保证没有在VPN集中器的现有配置。

VPN集中器在快速配置方面出现，并且这些项目在重新启动以后配置：

- 时间/日期
- 接口/掩码在**Configuration > Interfaces** (public=200.1.1.2/24， private=192.168.10.1/24)
- 在**Configuration > System** > IP Routing > **Default_Gateway** (200.1.1.1)的默认网关

这时， VPN集中器通过从网络内部的HTML是可取得。

注意： 由于VPN集中器从外面被管理，您必须也选择：

- **Configuration > Interfaces** > 2**公共>选择IP过滤器> 1.私有(默认)**。
- **Administration > Access Rights > Access Control List** > Add Manager Workstation添加*外部管理器的*IP地址。

除非管理VPN集中器从*外面*，这不是必要的。

1. 在您启动GUI后，请选择**Configuration > Interfaces**复校接口。
2. 选择**Configuration > System** > IP Routing > Default Gateways配置**默认**(互联网)**网关**和**通道默认**(里面)**网关**IPsec的能到达其他子网在私有网络。
3. 选择**Configuration > Policy Management** > Network Lists建立定义了将加密的流量的网络列表。这些是本地网络：这些是远程网络：
4. 当完成，这些是两张网络列表：**注意：** 如果IPSec隧道不出来，检查发现关注数据流是否在两边配比。关注数据流由在路由器和PIX方框的访问列表定义。他们由在VPN集中器的网络列表定义。
5. 选择**Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN**并且定义LAN-to-LAN隧道。
6. 在您单击后请**应用**，此窗口显示与由于LAN到LAN隧道配置，自动地创建的另一配置。创建的LAN对LAN IPSec参数在**Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN**可以以前被查看或修改。
7. 选择**Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**确认活动IKE建议。
8. 选择**Configuration > Policy Management > Traffic Management > Security Associations**查看安全关联列表。
9. 点击安全关联名称，然后单击**修改**验证安全关联。

验证

此部分列出用于此配置的**显示**命令。

在路由器上

本部分提供的信息可帮助您确认您的配置是否可正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输

出的分析。

- **show crypto ipsec sa** — 显示当前安全关联所使用的设置。
- **show crypto isakmp sa** - 显示对等体上的所有当前 Internet 密钥交换安全关联。
- **show crypto engine connection active** —表示所有加密引擎的当前活动加密的会话连接。

您能使用IOS命令查找工具(仅限注册用户)发现关于特定命令的更多信息。

在 VPN 集中器上

选择**Configuration > System > Events > Classes > Modify**启用登录。这些选项是可用的：

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

对Log=1-13的严重性

Console的严重性=1-3

选择**Monitoring > Event Log**检索事件日志。

故障排除

在路由器上

关于调试指令的参考的重要信息，在您尝试所有调试指令前。

- **debug crypto engine** - 显示已加密的流量。
- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** - 显示第 1 阶段的 ISAKMP 协商。

问题-无法发起通道

错误消息

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
```

```
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask 255.255.255.0
ip nat inside source route-map nonat pool mypool overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

解决方案

完成此操作为了配置同时登录所需的数量或设置同时登录到5此SA的：

去Configuration > User Management > Groups > Modify 10.19.187.229 >General > Simultaneouts登录并且更改登录数量到5。

PFS

在 IPsec 协商中，完全转发保密 (PFS) 可确保每个新的加密密钥与任何先前密钥不相关。请启用或禁用在两个隧道对等体的PFS。否则， LAN对LAN (L2L) IPSec隧道在路由器没有设立。

为了指定IPsec应该请求PFS，当新的安全关联为此加密映射项时请求，或者IPsec要求PFS，当收到要求新的安全关联，请使用**set pfs命令**在加密映射配置模式。为了指定IPsec不应该请求PFS，请使用此命令**no表示**。

```
set pfs [group1 | group2]
no set pfs
```

对于 set pfs 命令：

- *group1* —指定IPsec应该使用768-bit Diffie-Hellman最初模数组，当新的Diffie-Hellman交换进行。
- *第2组*—指定IPsec应该使用1024位Diffie-Hellman最初模数组，当新的Diffie-Hellman交换进行。

默认情况下，不会请求 PFS。如果使用此命令时未指定任何组，则 group1 会用作默认值。

示例：

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

参考Cisco IOS安全命令参考关于**set pfs命令的更多信息**。

相关信息

- 最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案
- Cisco VPN 3000 系列集中器
- Cisco VPN 3002 硬件客户端
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems