在拥有重复 LAN 子网的路由器之间配置 IPSec 隧道

目录

简介

本文提供网络示例模拟合并具有相同IP编址方案的两家公司。两个路由器用VPN通道连接，并且在每个路由器背后的网络是相同的。使一个站点访问在另一个站点的主机，网络地址转换(NAT)在路由器上用于更改源和目的地址为不同的子网。

注意： 从网络管理的角度考虑，此配置不推荐作为一个永久性设置。

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：

- 路由器A ：运行Cisco IOS软件版本12.3(4)T的Cisco 3640路由器
- 路由器B ：运行Cisco IOS软件版本12.3(5)的Cisco 2621路由器

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。

背景信息

在本例中，当在站点A的主机172.16.1.2访问在站点B同一IP地址的一台主机时，它连接到172.19.1.2地址而不是到实际的地址172.16.1.2。当在站点B的主机访问站点A，它连接到地址172.18.1.2。在路由器A上的NAT转换所有172.16.x.x地址，看起来匹配172.18.x.x主机条目。在路由器B上的NAT更改172.16.x.x看起来象172.19.x.x。

在每个路由器的加密功能加密经转换的流量通过串口。**注意NAT在路由器的加密前发生。**

注意： 此配置只允许两个网络通信。**它不允许Internet连接。**您需要另外的路径到互联网，以联通除两个站点之外位置;换句话说，您在需要添加另一个路由器或防火墙在每一侧，在主机上配置数个路由。

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： 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- 路由器 A
- 路由器 B

路由器 A

```
Current configuration : 1404 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
```

```
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- These are the Internet Key Exchange (IKE)
parameters. crypto isakmp policy 10 encr 3des hash md5
authentication pre-share crypto isakmp key cisco123
address 10.5.76.57 ! !--- These are the IPSec
parameters. crypto ipsec transform-set myset1 esp-3des
esp-md5-hmac ! ! crypto map mymap 10 ipsec-isakmp set
peer 10.5.76.57 set transform-set myset1 !--- Encrypt
traffic to the other side. match address 100 ! ! !
interface Serial0/0 description Interface to Internet ip
address 10.5.76.58 255.255.0.0 ip nat outside clockrate
128000 crypto map mymap ! interface Ethernet0/0 ip
address 172.16.1.1 255.255.255.0 no ip directed-
broadcast ip nat inside half-duplex ! ! !--- This is the
NAT traffic. ip nat inside source static network
172.16.0.0 172.18.0.0 /16 no-alias ip http server no ip
http secure-server ip classless ip route 0.0.0.0 0.0.0.0
Serial0/0 ! !--- Encrypt traffic to the other side.
access-list 100 permit ip 172.18.0.0 0.0.255.255
172.19.0.0 0.0.255.255 ! control-plane ! ! line con 0
line aux 0 line vty 0 4 ! ! end
```

路由器 B

```
Current configuration : 1255 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-15
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
no aaa new-model
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!--- These are the IKE parameters. crypto isakmp policy
10 encr 3des hash md5 authentication pre-share crypto
isakmp key cisco123 address 10.5.76.58 ! !--- These are
the IPSec parameters. crypto ipsec transform-set myset1
esp-3des esp-md5-hmac ! crypto map mymap 10 ipsec-isakmp
set peer 10.5.76.58 set transform-set myset1 !---
Encrypt traffic to the other side. match address 100 ! !
interface FastEthernet0/0 ip address 172.16.1.1
255.255.255.0 ip nat inside duplex auto speed auto !
interface Serial0/0 description Interface to Internet ip
address 10.5.76.57 255.255.0.0 ip nat outside crypto map
mymap ! !--- This is the NAT traffic. ip nat inside
```

```
source static network 172.16.0.0 172.19.0.0 /16 no-alias
ip http server no ip http secure-server ip classless ip
route 0.0.0.0 0.0.0.0 Serial0/0 ! !--- Encrypt traffic
to the other side. access-list 100 permit ip 172.19.0.0
0.0.255.255 172.18.0.0 0.0.255.255 ! ! line con 0 line
aux 0 line vty 0 4 ! ! ! end
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- **show crypto ipsec sa** — 显示第 2 阶段安全连接。
- **show crypto isakmp sa** - 显示第 1 阶段的安全关联。
- **show ip nat translation** -显示当前在使用中的NAT转换。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

注意： 在发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** - 显示第 1 阶段的 Internet 安全连接和密钥管理协议 (ISAKMP) 协商。
- **debug crypto engine** - 显示已加密的数据流。

相关信息

- IPSec 支持页面
- 配置 IPSec 网络安全
- 配置 Internet 密钥交换安全协议
- 技术支持 - Cisco Systems