# 在 IOS 路由器上采用隧道分离技术以 NEM 模式下配置 EzVPN 的配置示例

## 目录



## 简介

此配置详细说明了 Cisco IOS® 软件版本 12.3(11)T 中的新功能，通过该功能可以在同一个接口上将一个路由器配置为 EzVPN 客户端和服务器。数据流可以从 VPN 客户端被路由到 EzVPN 服务器，然后退出到另一个远程 EzVPN 服务器。

请参阅配置 IPsec 路由器动态 LAN 到 LAN 对等体和 VPN 客户端以了解有关以下方案的详细信息：在一个星型环境中的两个路由器之间存在 LAN 到 LAN 配置，其中 Cisco VPN 客户端也连接到中心，并使用了扩展验证 (XAUTH)。

有关 Cisco 871 路由器和 Cisco 7200 VXR 路由器之间 NEM 模式的 EzVPN 的示例配置，请参阅 7200 Easy VPN 服务器到 871 Easy VPN 远端客户端配置示例。

## 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：

- EzVPN 客户端和服务器路由器上的 Cisco IOS 软件版本 12.3(11)T。
- 远程 EzVPN 服务器路由器上的 Cisco IOS 软件版本 12.3(6)（这可以是支持 EzVPN 服务器功

能的任何加密版本）。
- Cisco VPN Client 版本 4.x

**注意：** 本文档文已经过 Cisco 3640 路由器和 Cisco IOS 软件版本 12.4(8) 再认证。

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：** 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

## 网络图

在此网络图中，RouterA 被同时配置为 EzVPN 客户端和服务器。这允许它接受来自 VPN 客户端的连接并允许它在连接到 RouterB 时充当 EzVPN 客户端。来自 VPN 客户端的数据流可被路由到 RouterA 和 RouterB 后的网络。

## 配置

必须使用 IPsec 配置文件配置 RouterA 才能进行 VPN 客户端连接。在此路由器上使用标准 EzVPN 服务器配置和 EzVPN 客户端配置无法工作。路由器在第 1 阶段协商期间发生故障。

在此示例配置中，RouterB 向 RouterA 发送一个 10.0.0.0/8 分割隧道列表。使用此配置，VPN 客户端池不能是 10.x.x.x 超网中的任何部分。什么发生是路由器A构件SA对流量的路由器B从10.1.1.0/24到10.0.0.0/8。为例，假设您让一VPN客户端连接和使IP地址脱离10.3.3.1的本地池。RouterA 为从 10.1.1.0/24 到 10.3.3.1/32 的数据流成功构建另一个 SA。但是，当来自 VPN 客户端的数据包被回复然后到达 RouterA 时，RouterA 将通过隧道将它们发送到 RouterB。这是因为它们匹配其 SA 10.1.1.0/24 到 10.0.0.0/8，而不是更精确的匹配 10.3.3.1/32。

您必须同时在 RouterB 上配置分割隧道。否则，VPN 客户端数据流无法工作。如果未定义分割隧道（在本示例中为 RouterB 上的 acl 150），RouterA 将为从 10.1.1.0/24 到 0.0.0.0/0 的数据流（所有数据流）构建一个 SA。当 VPN 客户端连接并收到任何池中的任何 IP 地址时，将始终通过隧道将返回它的数据流发送到 RouterB。这是因为首先匹配的是 RouterB。由于此 SA 定义了“所有数据流”，因此不管您的 VPN 客户端地址池如何，数据流都不会返回到它。

总之，您必须使用分割隧道，并且您的 VPN 地址池必须是不同于分割隧道列表中任何网络的超网。

本文档使用以下配置：

- 路由器A
- 路由器B

| **路由器A** |
| --- |

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable password cisco
!
username glenn password 0 cisco123
no network-clock-participate slot 1
no network-clock-participate wic 0
aaa new-model
!
!
aaa authentication login userlist local aaa
authorization network groupauthor local aaa session-id
common ip subnet-zero ip cef ! ip dhcp-server
172.17.81.127 ! ! crypto isakmp policy 1 encr 3des
authentication pre-share group 2 ! crypto isakmp
keepalive 20 10 ! !--- Group definition for the EzVPN
server feature. !--- VPN Clients that connect in need to
be defined with this !--- group name/password and are
allocated these attributes. crypto isakmp client
configuration group VPNCLIENTGROUP key mnbvcxz domain
nuplex.com.au pool vpn1 acl 150 ! ! !--- IPsec profile
for VPN Clients. crypto isakmp profile VPNclient
description VPN clients profile match identity group
VPNCLIENTGROUP client authentication list userlist
isakmp authorization list groupauthor client
configuration address respond ! ! crypto ipsec
transform-set 3des esp-3des esp-sha-hmac ! ! !---
Configuration for EzVPN Client configuration. These
parameters !--- are configured on RouterB. ACL 120 is
the new "multiple-subnet" !--- feature of EzVPN. This
allows the router to build an additional !--- SA for
traffic that matches the line in ACL 120 so that traffic
!--- from VPN Clients are routed over the EzVPN Client
tunnel !--- to RouterB. Without this, VPN Clients are
only able to !--- connect to subnets behind RouterA, and
not RouterB. crypto ipsec client ezvpn china connect
auto group china key mnbvcxz mode network-extension peer
10.66.79.105 acl 120 ! ! crypto dynamic-map SDM_CMAP_1
99 set transform-set 3des set isakmp-profile VPNclient
reverse-route ! ! crypto map SDM_CMAP_1 99 ipsec-isakmp
dynamic SDM_CMAP_1 ! ! ! interface FastEthernet0/0
description Outside interface ip address 10.66.79.102
255.255.255.224 ip nat outside ip virtual-reassembly
duplex auto speed auto crypto map SDM_CMAP_1 crypto
ipsec client ezvpn china ! ! interface FastEthernet1/0
description Inside interface ip address 10.1.1.1
255.255.255.0 ip nat inside ip virtual-reassembly duplex
auto speed auto crypto ipsec client ezvpn china inside !
! !--- IP pool of addresses. Note that this pool must be
!--- a different supernet to any of the split tunnel !--
- networks sent down from RouterB. ip local pool vpn1
192.168.1.1 192.168.1.254 ip classless ip route 0.0.0.0
0.0.0.0 10.66.79.97 ! no ip http server no ip http
secure-server ip nat inside source list 100 interface
FastEthernet0/0 overload ! access-list 100 deny ip
```

```
10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255 access-list 100
permit ip 10.1.1.0 0.0.0.255 any !--- Access-list that
defines additional SAs for this !--- router to create to
the head-end EzVPN server (RouterB). !--- Without this,
RouterA only builds an SA for traffic !--- from 10.1.1.0
to 10.2.2.0. VPN Clients !--- that connect (and get a
192.168.1.0 address) !--- are not able to get to
10.2.2.0. access-list 120 permit ip 192.168.1.0
0.0.0.255 10.0.0.0 0.255.255.255 !--- Split tunnel
access-list for VPN Clients. access-list 150 permit ip
10.1.1.0 0.0.0.255 any access-list 150 permit ip
10.2.2.0 0.0.0.255 any dialer-list 1 protocol ip permit
! ! control-plane ! ! ! ! line con 0 exec-timeout 0 0
login authentication nada line aux 0 modem InOut modem
autoconfigure type usr_courier transport input all speed
38400 line vty 0 4 transport preferred all transport
input all ! ! end
```

**路由器B**

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
!
aaa new-model
!
!
!--- No XAuth is defined but can be if needed. aaa
authorization network groupauthor local aaa session-id
common ip subnet-zero ip cef ! ! ! crypto isakmp policy
1 encr 3des authentication pre-share group 2 crypto
isakmp keepalive 10 ! ! !--- Standard EzVPN server
configuration, !--- matching parameters defined on
RouterA. crypto isakmp client configuration group china
key mnbvcxz acl 150 ! ! crypto ipsec transform-set 3des
esp-3des esp-sha-hmac ! crypto dynamic-map dynmap 1 set
transform-set 3des reverse-route ! ! ! crypto map mymap
isakmp authorization list groupauthor crypto map mymap
client configuration address respond crypto map mymap 10
ipsec-isakmp dynamic dynmap ! ! ! ! interface
Ethernet0/0 description Outside interface ip address
10.66.79.105 255.255.255.224 half-duplex crypto map
mymap ! ! interface Ethernet0/1 description Inside
interface ip address 10.2.2.1 255.255.255.0 half-duplex
! no ip http server no ip http secure-server ip
classless ip route 0.0.0.0 0.0.0.0 10.66.79.97 ! !
access-list 150 permit ip 10.0.0.0 0.255.255.255 any ! !
line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 ! !
! end
```

## VPN 客户端配置

创建一个引用路由器 RouterA 的 IP 地址的新连接条目。在本示例中，组名是“VPNCLIENTGROUP”，口令是“mnbvcxz”，可以在路由器配置中看到。

# 验证与故障排除

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。有关其他验证/故障排除信息，请参阅 IP 安全故障排除 - 了解和使用 debug 命令。如果遇到任何 VPN 客户端问题或错误，请参阅 VPN 客户端 GUI 错误查找工具。

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。

# 相关信息

- **IPSec 配置文件配置**
- **Cisco VPN 客户端支持页**
- **IPsec 协商/IKE 协议支持页**
- **技术支持和文档 - Cisco Systems**