在IOS路由器上使用分割隧道的NEM模式的EzVPN配置示例

目錄

簡介

此配置詳細介紹Cisco IOS®軟體版本12.3(11)T中的新功能，通過該功能，可以將路由器配置為EzVPN客戶端和同一介面上的伺服器。流量可以從VPN客戶端路由到EzVPN伺服器，然後返回到另一個遠端EzVPN伺服器。

請參閱設定IPsec路由器動態LAN到LAN對等路由器和VPN客戶端，以瞭解更多有關在中心輻射環境中的兩台路由器之間存在LAN到LAN配置的場景，其中Cisco VPN客戶端也連線到集線器且使用擴展身份驗證(XAUTH)。

有關在Cisco 871路由器與具有NEM模式的Cisco 7200VXR路由器之間的EzVPN配置示例，請參閱7200 Easy VPN Server to 871 Easy VPN Remote配置示例。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- EzVPN客戶端和伺服器路由器上的Cisco IOS軟體版本12.3(11)T。
- 遠端EzVPN伺服器路由器上的Cisco IOS軟體版本12.3(6)（可以是支援EzVPN伺服器功能的任

何加密版本）。
- Cisco VPN使用者端版本4.x

注意：本文是使用Cisco IOS軟體版本12.4(8)的Cisco 3640路由器重新認證的。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

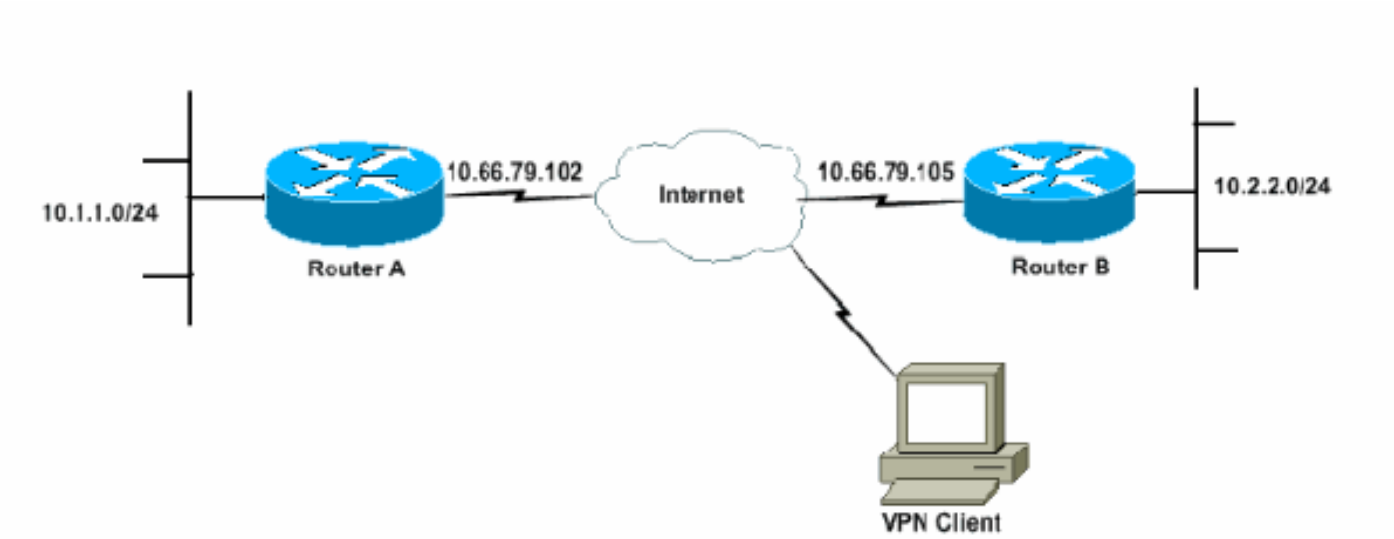
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

在此網路圖中，RouterA設定為EzVPN使用者端和伺服器。這允許它接受來自VPN客戶端的連線，並在連線到RouterB時充當EzVPN客戶端。來自VPN客戶端的流量可以路由到RouterA和RouterB後面的網路。



組態

必須為VPN客戶端連線配置RouterA的IPsec配置檔案。在此路由器上使用標準EzVPN伺服器配置以及EzVPN客戶端配置不起作用。路由器在第1階段協商失敗。

在此組態範例中，RouterB將10.0.0.0/8分隔通道清單傳送到RouterA。通過此配置，VPN客戶端池不能是10.x.x.x超網中的任何內容。發生的情況是，RouterA為從10.1.1.0/24到10.0.0.0/8的流量建立到RouterB的SA。例如，假設您有一個VPN客戶端連線，並從本地池10.3.3.1獲取IP地址。RouterA成功為從10.1.1.0/24到10.3.3.1/32的流量建立另一個SA。但是，當從VPN客戶端收到的資料包被回覆然後命中RouterA時，RouterA會通過隧道將它們傳送到RouterB。這是因為它們匹配其SA 10.1.1.0/24到10.0.0.0/8，而不是更具體的匹配項10.3.3.1/32。

您還必須在RouterB上設定分割通道。否則，VPN客戶端流量將永遠無法正常工作。如果沒有定義分割通道（本例中為RouterB上的acl 150），RouterA會為從10.1.1.0/24到0.0.0.0/0的流量（所有流量）建立一個SA。 當VPN客戶端連線並從任何池接收任何IP地址時，其返回流量始終通過隧道傳送到RouterB。這是因為它先被匹配。由於此SA定義了「所有流量」，因此無論您的VPN客戶端地址池是什麼，流量永遠不會返回到它。

總之，您必須使用拆分隧道，並且VPN地址池必須與拆分隧道清單中的任何網路不同。

本檔案會使用以下設定：

- 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

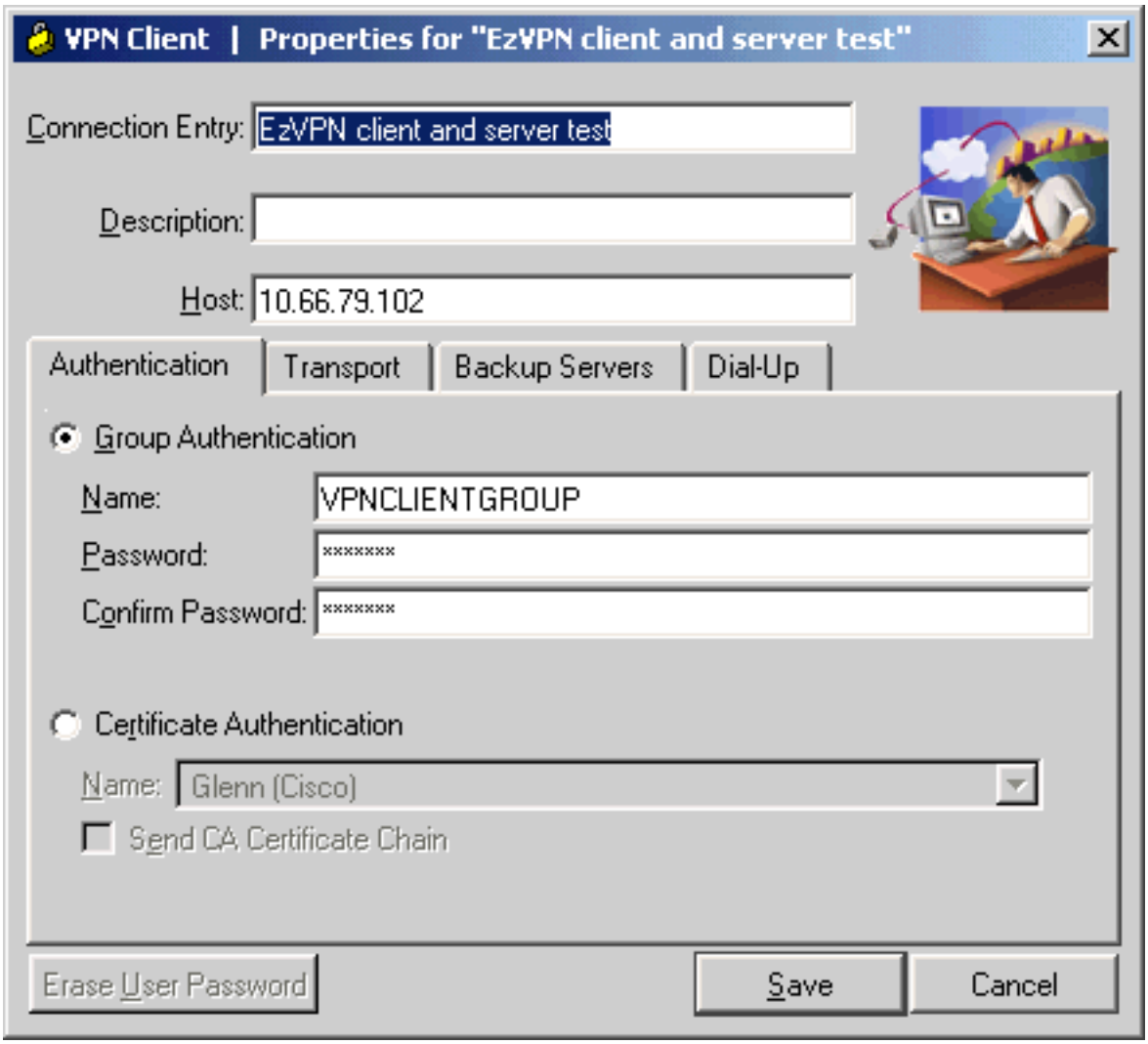
```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
!
aaa new-model
```

```
!
!
!--- 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客戶端配置

建立一個引用路由器RouterA的IP地址的新連線條目。此範例中的群組名稱為「VPNCLIENTGROUP」，密碼為「mnbvcxz」，這在路由器組態中可看到。



驗證和疑難排解

本節提供的資訊可用於確認您的組態是否正常運作。請參閱IP安全性疑難排解 — 瞭解和使用debug命令以瞭解其他驗證/疑難排解資訊。如果遇到任何VPN客戶端問題或錯誤，請參閱VPN客戶端GUI錯誤查詢工具。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

相關資訊

- IPsec設定檔組態

- Cisco VPN使用者端支援頁面
- IPsec協商/IKE通訊協定支援頁面
- 技術支援與文件 - Cisco Systems