

# 使用RIP和CVC在Cisco IOS路由器和VPN 5000集中器之間配置GRE Over IPsec

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[疑難排解指令](#)

[相關資訊](#)

## 簡介

此配置示例說明如何在Cisco VPN 5000集中器和Cisco IOS®路由器之間通過IPsec配置通用路由封裝(GRE)。VPN 5000 Concentrator 6.0(19)軟體版本中引入了GRE-over-IPsec功能。

在此示例中，路由資訊協定(RIP)用作動態路由協定，通過VPN隧道路由流量。

## 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：

- Cisco IOS軟體版本12.1(5)T7
- VPN 5000 Concentrator軟體版本6.0(19)

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

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

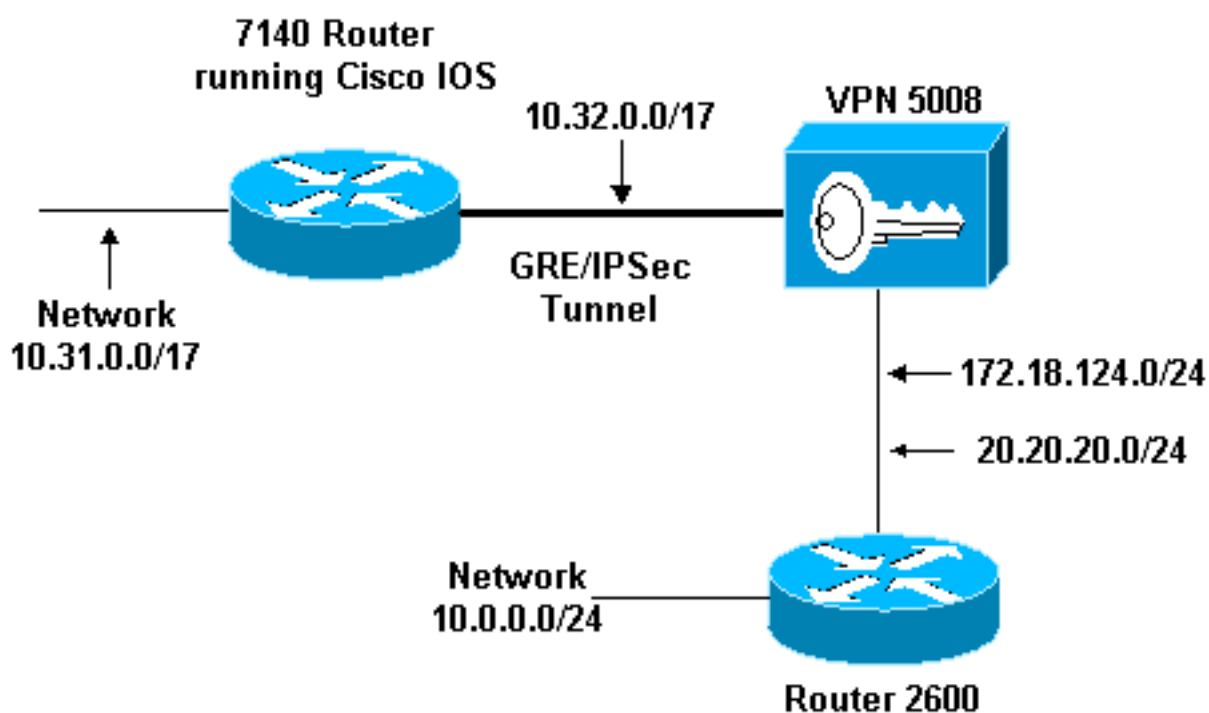
## 設定

本節提供用於設定本文件中所述功能的資訊。

**注意：**要查詢有關本文檔中使用的命令的其他資訊，請使用[命令查詢工具](#)([僅限註冊客戶](#))。

## 網路圖表

本檔案會使用下圖中所示的網路設定。



GRE over IPsec在Cisco IOS路由器(7140)和Cisco VPN 5008集中器之間配置。在這些裝置後面，通過RIP通告多個網路，RIP在7140和VPN 5008之間的GRE隧道內運行。

Cisco 7140背後的網路包括：

- 10.31.0.0/17

VPN 5008背後的網路包括：

- 172.18.124.0.0/24
- 20.20.20.0/24
- 10.0.0.0/24

## 組態

本文檔使用此處顯示的配置。

- [Cisco IOS路由器](#)
- [VPN 5000 Concentrator](#)
- [CVC](#)

## Cisco IOS路由器

```

Building configuration...

Current configuration : 1607 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 03-vpn-7140
!
boot system flash disk1:c7100-ik8s-mz.122-3
logging rate-limit console 10 except errors
enable password <removed>
!
ip subnet-zero
ip cef
!
!
no ip finger
!
! !--- Define phase 1 policy. crypto isakmp policy 10
authentication pre-share
!--- Define the PreShared Key for the Remote peer !---
(5000 ) in this example. crypto isakmp key cisco123
address 10.32.1.161
!
!--- Define Phase 2 policy. !--- Make sure that
Transport Mode is enabled. crypto ipsec transform-set
www esp-des esp-sha-hmac
mode transport
!
!--- Define the crypto map that is later !--- applied on
the outbound interface. crypto map temp 10 ipsec-isakmp
set peer 10.32.1.161
set transform-set www
match address 100
!
call rsvp-sync
!
!
!
!
!
!
!
controller ISA 5/1
!
!--- Define the GRE tunnel on the router. !--- Tunnel
source is the outbound interface !--- and tunnel
destination is VPN 5000. interface Tunnel0
ip address 10.1.1.2 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination 10.32.1.161
crypto map temp

```

```

!
!--- Outbound Interface that is connected to the
Internet. interface FastEthernet0/0
ip address 10.32.1.162 255.255.128.0
duplex auto
speed auto
crypto map temp
!
!!-- Inside interface. interface FastEthernet0/1 ip
address 10.31.100.1 255.255.128.0 no keepalive duplex
auto speed auto ! interface Serial1/0 no ip address
shutdown framing c-bit cablelength 10 dsu bandwidth
44210 ! interface Serial1/1 no ip address shutdown
framing c-bit cablelength 10 dsu bandwidth 44210 ! !---
Define RIP Routing Protocol on the router. !--- This
example shows Version 2 for classless routing. router
rip
version 2
network 10.0.0.0
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.32.1.1
no ip http server
!
!--- Encryption access-list that is used !--- to encrypt
the GRE packets. access-list 100 permit gre host
10.32.1.162 host 10.32.1.161
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 5 15
!
end

```

## VPN 5000 Concentrator

### show configuration

Edited Configuration not Present, using Running

[ IP Ethernet 0:0 ]

SubnetMask = 255.255.255.0

IPAddress = 1.1.1.1

[ IP Ethernet 1:0 ]Mode = Routed

SubnetMask = 255.255.128.0

IPAddress = 10.32.1.161

[ General ]

VPNGateway = 10.32.1.1

EnablePassword = <removed>

Password = <removed>

EthernetAddress = 00:00:a5:e9:c8:00

DeviceType = VPN 5002/8 Concentrator

ConfiguredOn = Timeserver not configured

ConfiguredFrom = Command Line, from Console

[ IKE Policy ]

Protection = SHA\_DES\_G1

```
[ IP Static ]
0.0.0.0 0.0.0.0 10.32.1.1 1 redist=none

[ Context List ]
flash://rip.cfg

[ Logging ]
Enabled = On
Level = 7

Configuration size is 822 out of 65500 bytes.
VPN5002_8_A5E9C800: Main#
```

## CVC

### **show configuration**

Edited Configuration not Present, using Running

```
[ General ]
Context = "rip"

[ IP Ethernet 1:0.1 ]
VLANID = 124
Encapsulation = dot1q
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 172.18.124.219

[ IP Static ]

[ Tunnel Partner VPN 1 ]
InactivityTimeout = 120
Transform = esp sha,des
KeyManage = ReliablePeer = "10.31.0.0/17"
LocalAccess = "10.5.1.0/24"
SharedKey = "cisco123"
Mode = Main
TunnelType = GREinIPSec
BindTo = "Ethernet 1:0"
Partner = 10.32.1.162

[ IP VPN 1 ]
RIPIn = On
RIPOut = On
RIPVersion = V2
DirectedBroadcast = Off
Numbered = On
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 10.1.1.1

[ IP Ethernet 1:0.2 ]
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 20.20.20.20
```

Configuration size is 1127 out of 65500 bytes.

VPN5002\_8\_A5E9C800: rip#

## 驗證

本節提供的資訊可用於確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

- **show ip route** — 顯示路由表的當前狀態。
- **show crypto engine connection active** — 顯示每個IPSec安全關聯的資料包加密/解密計數器。
- **show crypto ipsec sa** — 顯示所有當前IPSec安全關聯。
- **show system log buffer** — 顯示基本系統日誌資訊。
- **vpn trace dump** — 顯示有關VPN進程的詳細資訊。

```
03-vpn-7140#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is 10.32.1.1 to network 0.0.0.0
```

```
20.0.0.0/24 is subnetted, 1 subnets
```

```
R 20.20.20.0 [120/1] via 10.1.1.1, 00:00:10, Tunnel0
```

```
172.18.0.0/16 is variably subnetted, 2 subnets, 2 masks
```

```
R 172.18.124.0/24 [120/1] via 10.1.1.1, 00:00:10, Tunnel0
```

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
```

```
R 10.0.0.0/24 [120/2] via 10.1.1.1, 00:00:10, Tunnel0
```

```
C 10.1.1.0/24 is directly connected, Tunnel0
```

```
C 10.31.0.0/17 is directly connected, FastEthernet0/1
```

```
C 10.32.0.0/17 is directly connected, FastEthernet0/0
```

```
S* 0.0.0.0/0 [1/0] via 10.32.1.1
```

```
03-vpn-7140#
```

```
03-vpn-7140#show crypto enggine connection active
```

```
ID Interface IP-Address State Algorithm Encrypt Decrypt
3 FastEthernet0/0 10.32.1.162 set HMAC_SHA+DES_56_CB 0 0
4 FastEthernet0/0 10.32.1.162 set HMAC_SHA+DES_56_CB 0 0
5 FastEthernet0/0 10.32.1.162 set HMAC_SHA+DES_56_CB 0 0
2098 FastEthernet0/0 10.32.1.162 set HMAC_SHA+DES_56_CB 0 1892
2099 FastEthernet0/0 10.32.1.162 set HMAC_SHA+DES_56_CB 11552 0
```

```
03-vpn-7140#show crypto ipsec sa
```

```
interface: FastEthernet0/0
```

```
Crypto map tag: temp, local addr. 10.32.1.162
```

```
local ident (addr/mask/prot/port): (10.32.1.162/255.255.255.255/0/0)
```

```
remote ident (addr/mask/prot/port): (10.32.1.161/255.255.255.255/0/0)
```

```
current_peer: 10.32.1.161
```

```
PERMIT, flags={transport_parent,}
```

```
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
```

```
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
```

#send errors 0, #recv errors 0

local crypto endpt.: 10.32.1.162, remote crypto endpt.: 10.32.1.161  
path mtu 1500, media mtu 1500  
current outbound spi: 0

inbound esp sas:

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

outbound ah sas:

outbound pcsp sas:

local ident (addr/mask/prot/port): (10.32.1.162/255.255.255.255/47/0)  
remote ident (addr/mask/prot/port): (10.32.1.161/255.255.255.255/47/0)  
current\_peer: 10.32.1.161  
PERMIT, flags={origin\_is\_acl,transport\_parent,}  
**#pkts encaps: 12912, #pkts encrypt: 12912, #pkts digest 12912**  
**#pkts decaps: 2382, #pkts decrypt: 2382, #pkts verify 2382**  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0  
#send errors 0, #recv errors 0

local crypto endpt.: 10.32.1.162, remote crypto endpt.: 10.32.1.161  
path mtu 1500, media mtu 1500  
current outbound spi: 101

inbound esp sas:

spi: 0x4624F3AD(1176826797)  
transform: esp-des esp-sha-hmac ,  
in use settings = {Transport, }  
slot: 0, conn id: 2098, flow\_id: 69, crypto map: temp

sa timing: remaining key lifetime (k/sec): (1048130/3179)  
IV size: 8 bytes  
replay detection support: Y

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

spi: 0x101(257)  
transform: esp-des esp-sha-hmac ,  
in use settings = {Transport, }  
slot: 0, conn id: 2099, flow\_id: 70, crypto map: temp  
sa timing: remaining key lifetime (k/sec): (1046566/3179)  
IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcsp sas:

```
interface: Tunnel0
Crypto map tag: temp, local addr. 10.32.1.162

local ident (addr/mask/prot/port): (10.32.1.162/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.32.1.161/255.255.255.255/0/0)
current_peer: 10.32.1.161
PERMIT, flags={transport_parent,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.32.1.162, remote crypto endpt.: 10.32.1.161
path mtu 1500, media mtu 1500
current outbound spi: 0

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

local ident (addr/mask/prot/port): (10.32.1.162/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (10.32.1.161/255.255.255.255/47/0)
current_peer: 10.32.1.161
PERMIT, flags={origin_is_acl,transport_parent,}
#pkts encaps: 13017, #pkts encrypt: 13017, #pkts digest 13017
#pkts decaps: 2410, #pkts decrypt: 2410, #pkts verify 2410
#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.32.1.162, remote crypto endpt.: 10.32.1.161
path mtu 1500, media mtu 1500
current outbound spi: 101

inbound esp sas:
spi: 0x4624F3AD(1176826797)
transform: esp-des esp-sha-hmac ,
in use settings ={Transport, }
slot: 0, conn id: 2098, flow_id: 69, crypto map: temp
sa timing: remaining key lifetime (k/sec): (1048124/3176)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x101(257)
transform: esp-des esp-sha-hmac ,
in use settings ={Transport, }
slot: 0, conn id: 2099, flow_id: 70, crypto map: temp
sa timing: remaining key lifetime (k/sec): (1046566/3176)
```



IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcp sas:

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

### 疑難排解指令

[輸出直譯器工具](#)(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

**注意：**發出debug指令之前，請先參閱[有關Debug指令的重要資訊](#)。

- **debug crypto isakmp**(Cisco IOS Router) — 顯示有關網際網路金鑰交換(IKE)第I階段 (主模式) 交涉的詳細資訊。
- **debug crypto ipsec**(Cisco IOS Router) — 顯示有關IKE第II階段 (快速模式) 協商的詳細資訊。
- **debug crypto engine**(Cisco IOS Router) — 調試封包加密/解密和Diffie-Hellman(DH)程式。
- **debug ip rip**(Cisco IOS路由器) — 調試RIP路由協定。

從VPN 5000集中器發出show ip routing命令。

```
VPN5002_8_A5E9C800: rip#show ip routing
```

```
IP Routing Table for rip
Directly Connected Routes:
Destination Mask Ref Uses Type Interface
10.1.1.0 FFFFFFF0 5 STIF VPN0:1
10.1.1.0 FFFFFFFF 0 STIF Local
10.1.1.1 @FFFFFFF 5 LocalLocal
10.1.1.255 FFFFFFFF 0 STIF Local
20.20.20.0 FFFFFFF0 1352 STIF Ether1:0.2
20.20.20.0 FFFFFFFF 0 STIF Local
20.20.20.20 @FFFFFFF 14 LocalLocal
20.20.20.255 FFFFFFFF 1318 STIF Local
127.0.0.1 FFFFFFFF 0 STIF Local
172.18.124.0 FFFFFFF0 13789 STIF Ether1:0.1
172.18.124.0 FFFFFFFF 0 STIF Local
172.18.124.219 @FFFFFFF 6 LocalLocal
172.18.124.255 FFFFFFFF 13547 STIF Local
224.0.0.5 FFFFFFFF 0 STIF Local
224.0.0.6 FFFFFFFF 0 STIF Local
224.0.0.9 FFFFFFFF 15 STIF Local
255.255.255.255 @FFFFFFF 221 LocalLocal

Static Routes:
Destination Mask Gateway Metric Ref Uses Type Interface
10.31.0.0 FFFF0000 Interface 1 0 Stat VPN0:1
10.32.1.162 @FFFFFFF 10.32.1.161 2 0 *Stat VPN0:1

Dynamic Routes:
Src/
Destination Mask Gateway Metric Ref Uses Type TTL Interface
DEFAULT 10.1.1.2 1 293 RIP2 165 VPN0:1
10.0.0.0 FFFFFFF0 172.18.124.216 1 0 RIP1 160 Ether1:0.1
```

```
10.31.0.0 FFFF8000 10.1.1.2 1 0 RIP2 165 VPN0:1
10.32.0.0 FFFF8000 10.1.1.2 1 0 RIP2 165 VPN0:1
```

Configured IP Routes:

```
Destination Mask Gateway Metric IFnum Flags
10.31.0.0 FFFF0000 Interface 1 VPN 0:1 Redist = none
```

Total Routes in use: 23 Mask -> @Host route Type -> Redist \*rip #ospf

VPN5002\_8\_A5E9C800: rip#**show vpn stat ver**

```
Current In High Running Script Script Script
Active Negot Water Total Starts OK Error
```

```
-----
Users 0 0 0 0 0 0 0
Partners 1 0 1 1 1 0 0
Total 1 0 1 1 1 0 0
```

Stats VPN0:1

**Wrapped 2697**  
**Unwrapped 14439**

```
BadEncap 0
BadAuth 0
BadEncrypt 0
rx IP 14439
rx IPX 0
rx Other 0
tx IP 2697
tx IPX 0
tx Other 0
IKE rekey 0
```

Input VPN pkts dropped due to no SA: 1

Input VPN pkts dropped due to no free queue entries: 0

IOP slot 1:

```
Current In High Running Script Script Script
Active Negot Water Total Starts OK Error
```

```
-----
Users 0 0 0 0 0 0 0
Partners 0 0 0 0 0 0 0
Total 0 0 0 0 0 0 0
```

Stats

```
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
```

IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

IOP slot 2:

Current In High Running Script Script Script  
Active Negot Water Total Starts OK Error

-----  
Users 0 0 0 0 0 0 0  
Partners 0 0 0 0 0 0 0  
Total 0 0 0 0 0 0 0

Stats  
Wrapped  
Unwrapped  
BadEncap  
BadAuth  
BadEncrypt  
rx IP  
rx IPX  
rx Other  
tx IP  
tx IPX  
tx Other  
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

IOP slot 3:

Current In High Running Script Script Script  
Active Negot Water Total Starts OK Error

-----  
Users 0 0 0 0 0 0 0  
Partners 0 0 0 0 0 0 0  
Total 0 0 0 0 0 0 0

Stats  
Wrapped  
Unwrapped  
BadEncap  
BadAuth  
BadEncrypt  
rx IP  
rx IPX  
rx Other  
tx IP  
tx IPX  
tx Other  
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

## [相關資訊](#)

- [Cisco VPN 5000系列集中器支援頁](#)
- [Cisco VPN 5000使用者端支援頁面](#)
- [IPSec \( IP 安全通訊協定 \) 支援頁面](#)
- [技術支援 - Cisco Systems](#)