

# Cisco IOS ルータとRIPおよびCVC を使用して VPN 5000 コンセントレータ 間のGRE Over IPSec を設定する方法

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

## 概要

この設定例では、Cisco VPN 5000コンセントレータとCisco IOS®ルータ間でGeneric Routing Encapsulation(GRE)over IPSecを設定する方法について説明します。GRE-over-IPSec 機能は、VPN 5000 コンセントレータ 6.0(19) ソフトウェア リリースに導入されています。

この例では、Routing Information Protocol(RIP)をダイナミックルーティングプロトコルとして使用して、トラフィックをVPNトンネル経由でルーティングします。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOSソフトウェアリリース12.1(5)T7
- VPN 5000 コンセントレータ ソフトウェア リリース 6.0(19)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

ドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 表記法

ドキュメントの表記法の詳細は、「[シスコ テクニカル ティップスの表記法](#)」を参照してください。

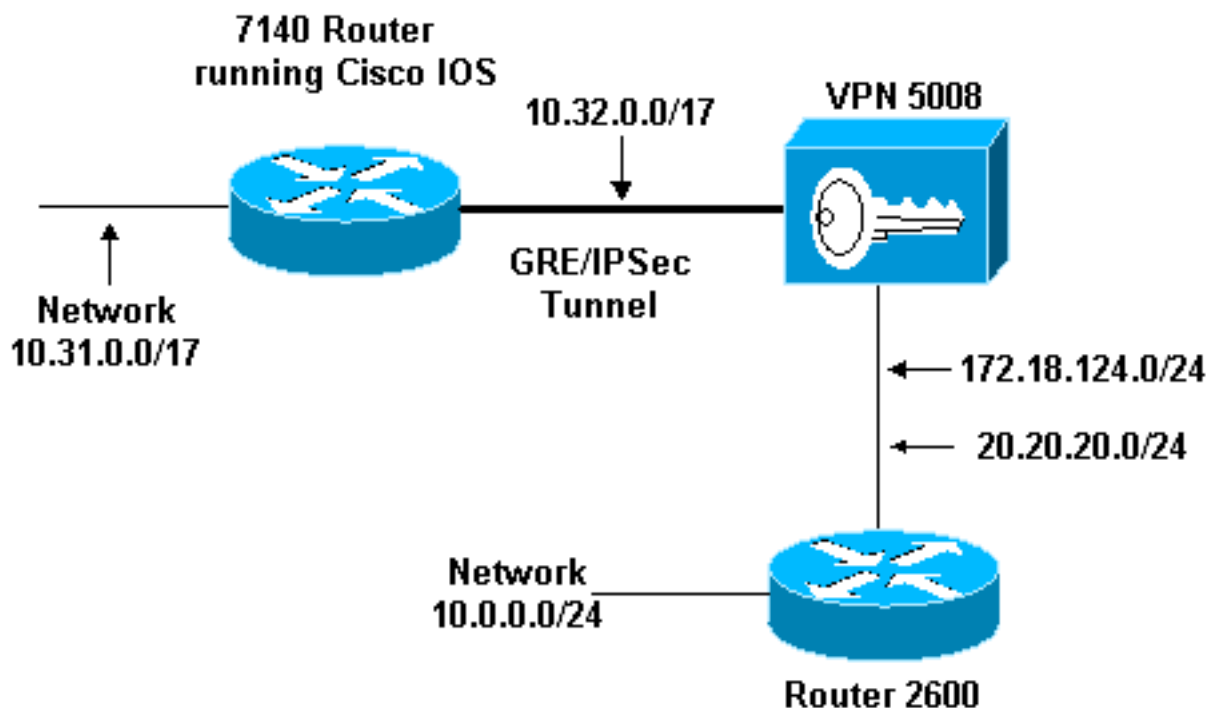
## 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください（登録ユーザーのみ）。

## ネットワーク図

このドキュメントでは、次の図で示されるネットワーク設定を使用しています。



GRE over IPsecは、Cisco IOSルータ(7140)とCisco VPN 5008コンセンレータの間で設定されます。これらのデバイスの背後では、7140とVPN 5008の間のGREトンネル内で実行されるRIPを介して複数のネットワークがアドバタイズされます。

Cisco 7140の背後にあるネットワークは次のとおりです。

- 10.31.0.0/17

VPN 5008の背後にあるネットワークは次のとおりです。

- 172.18.124.0/24
- 20.20.20.0/24
- 10.0.0.0/24

## 設定

このドキュメントでは、次に示す設定を使用しています。

- [Cisco IOS ルータ](#)
- [VPN 5000 コンセントレータ](#)
- [CVC](#)

### Cisco IOS ルータ

```
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 コンセントレータ

### 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 redistrib=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#
```

## 確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

一部の show コマンドは[アウトプット インタープリタ ツールによってサポートされています \( 登録ユーザ専用 \)](#)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- **show ip route** : ルーティングテーブルの現在の状態を表示します。
- **show crypto engine connection active**:IPSecセキュリティアソシエーションごとのパケット暗号化/復号化カウンタを表示します。
- **show crypto ipsec sa** : 現在のIPSecセキュリティアソシエーションをすべて表示します。
- **show system log buffer** : 基本的な Syslog 情報を表示します。
- **vpn trace dump** : VPN プロセスの詳細情報を表示します。

```
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 engine 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 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: 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 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): (1046566/3179)  
IV size: 8 bytes  
replay detection support: Y

outbound ah sas:

outbound pcp 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:

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

### トラブルシューティングのためのコマンド

一部の show コマンドは [アウトプット インタープリタ ツールによってサポートされています \(登録ユーザ専用\)](#)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

注： debug コマンドを使用する前に、「[debug コマンドに関する重要な情報](#)」を参照してください。

- **debug crypto isakmp** ( Cisco IOSルータ ) :Internet Key Exchange(IKE)フェーズI (メインモード) ネゴシエーションの詳細情報を表示します。
- **debug crypto ipsec** ( Cisco IOSルータ ) :IKEフェーズII (クイックモード) ネゴシエーションの詳細情報を表示します。
- **debug crypto engine** ( Cisco IOSルータ ) : パケットの暗号化/復号化およびDiffie-Hellman(DH)プロセスをデバッグします。
- **debug ip rip** ( Cisco IOSルータ ) :RIPルーティングプロトコルをデバッグします。

VPN 5000コンセンレータから **show ip routing** コマンドを発行します。

```
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 FFFFFFF00 1352 STIF Ether1:0.2
20.20.20.0 FFFFFFFF 0 STIF Local
20.20.20.20 @FFFFFFFF 14 LocalLocal
20.20.20.255 FFFFFFFF 1318 STIF Local
127.0.0.1 FFFFFFFF 0 STIF Local
172.18.124.0 FFFFFFF00 13789 STIF Ether1:0.1
172.18.124.0 FFFFFFFF 0 STIF Local
172.18.124.219 @FFFFFFFF 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 @FFFFFFFF 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 @FFFFFFFF 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 FFFFFFF00 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

## **関連情報**

- [Cisco VPN 5000 シリーズ コンセントレータに関するサポート ページ](#)
- [Cisco VPN 5000 クライアントに関するサポート ページ](#)
- [IPSec \( IP セキュリティ プロトコル \) に関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)