

Configurazione di GRE over IPSec tra un router Cisco IOS e un concentratore VPN 5000 con RIP e CVC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questa configurazione di esempio viene descritto come configurare GRE (Generic Routing Encapsulation) su IPSec tra un concentratore Cisco VPN 5000 e un router Cisco IOS®. La funzione GRE-over-IPSec è stata introdotta nel software VPN 5000 Concentrator 6.0(19).

In questo esempio, il protocollo RIP (Routing Information Protocol) viene utilizzato come protocollo di routing dinamico per indirizzare il traffico attraverso il tunnel VPN.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS release 12.1(5)T7
- Software VPN 5000 Concentrator release 6.0(19)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

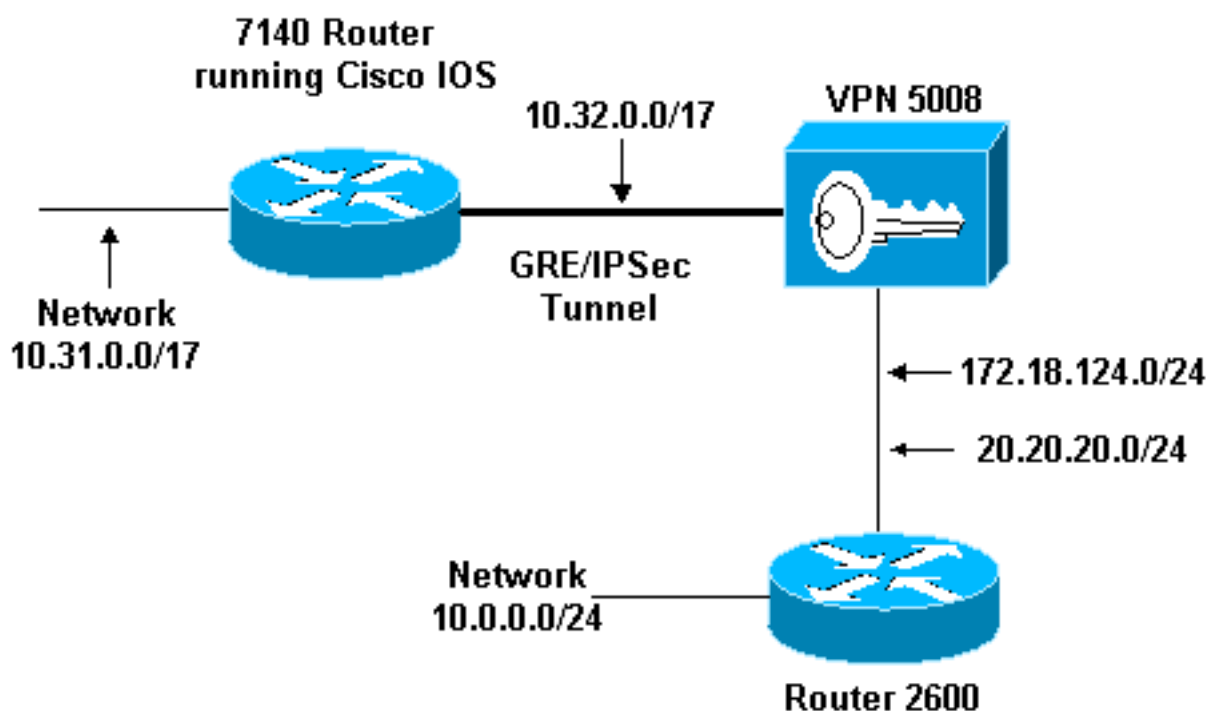
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Il protocollo GRE over IPsec è configurato tra il router Cisco IOS (7140) e Cisco VPN 5008 Concentrator. Dietro a questi dispositivi, più reti vengono pubblicizzate tramite RIP, che funziona all'interno del tunnel GRE tra 7140 e VPN 5008.

Le reti alla base di Cisco 7140 sono:

- 10.31.0.0/17

Le reti alla base di VPN 5008 sono:

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

Configurazioni

Nel documento vengono usate le configurazioni mostrate di seguito.

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

Cisco IOS Router

```
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 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#

```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- **show ip route**: visualizza lo stato corrente della tabella di routing.
- **show crypto engine connection active**: visualizza il contatore di crittografia/decrittografia dei pacchetti per associazione di protezione IPsec.
- **show crypto ipsec sa**: visualizza tutte le associazioni di protezione IPsec correnti.
- **show system log buffer**: visualizza le informazioni di base sul syslog.
- **vpn trace dump**: visualizza informazioni dettagliate sui processi VPN.

```
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 pcg 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 pcg 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 pcg sas:

outbound esp sas:

outbound ah sas:

outbound pcg 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:

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

Nota: prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#).

- **debug crypto isakmp** (Cisco IOS Router): visualizza informazioni dettagliate sulla negoziazione IKE (Internet Key Exchange) fase I (modalità principale).
- **debug crypto ipsec** (Cisco IOS Router): visualizza informazioni dettagliate sulla negoziazione IKE fase II (modalità rapida).
- **debug crypto engine** (Cisco IOS Router): esegue il debug del processo di crittografia/decrittografia dei pacchetti e di Diffie-Hellman (DH).
- **debug ip rip** (Cisco IOS Router): esegue il debug del protocollo di routing RIP.

Eseguire il comando **show ip routing** da VPN 5000 Concentrator.

```
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 @FFFFFFFF 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 @FFFFFFFF 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 @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 FFFFFF00 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

[Informazioni correlate](#)

- [Pagina di supporto per Cisco VPN serie 5000 concentrator](#)
- [Pagina di supporto per i client Cisco VPN 5000](#)
- [Pagina di supporto per IPSec \(IP Security Protocol\)](#)
- [Supporto tecnico – Cisco Systems](#)