RIP 및 CVC를 사용하여 Cisco IOS 라우터와 VPN 5000 Concentrator 간 GRE Over IPSec 구성

목차

소개

이 샘플 컨피그레이션에서는 Cisco VPN 5000 Concentrator와 Cisco IOS® 라우터 간에 IPSec을 통한 GRE(Generic Routing Encapsulation)를 구성하는 방법에 대해 설명합니다. GRE-over-IPSec 기능은 VPN 5000 Concentrator 6.0(19) 소프트웨어 릴리스에 도입되었습니다.

RIP(Routing Information Protocol)는 VPN 터널을 통해 트래픽을 라우팅하기 위해 이 샘플에서 동적 라우팅 프로토콜로 사용됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

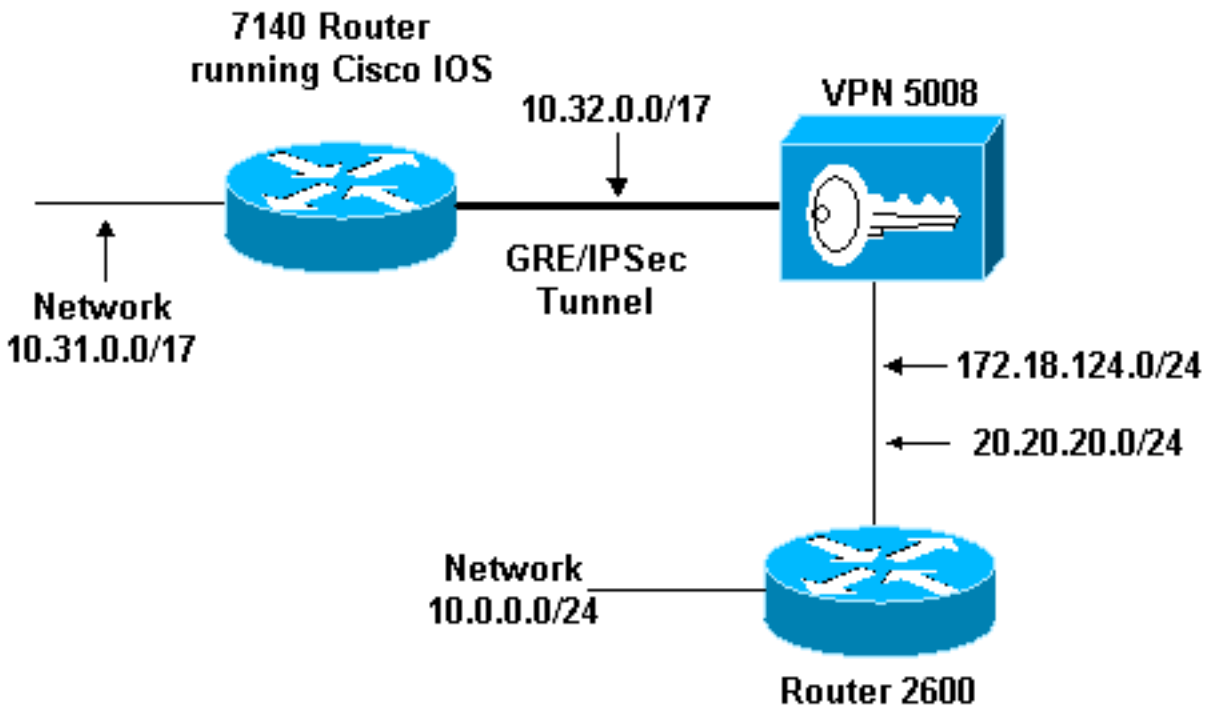
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



GRE over IPSec은 Cisco IOS 라우터(7140)와 Cisco VPN 5008 Concentrator 간에 구성됩니다. 이러한 디바이스 뒤에는 7140과 VPN 5008 사이의 GRE 터널 내에서 실행되는 RIP를 통해 여러 네트워크가 광고됩니다.

Cisco 7140을 지원하는 네트워크는 다음과 같습니다.

- 10.31.0.0/17

VPN 5008 뒤의 네트워크는 다음과 같습니다.

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

구성

이 문서에서는 여기에 표시된 구성을 사용합니다.

- Cisco IOS 라우터
- VPN 5000 Concentrator
- CVC

Cisco IOS 라우터

```
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#
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show ip route** - 라우팅 테이블의 현재 상태를 표시합니다.
- **show crypto engine connection active(암호화 엔진 연결 활성** 표시) - IPSec 보안 연결당 패킷 암호화/암호 해독 카운터를 표시합니다.
- **show crypto ipsec sa** - 현재 모든 IPSec 보안 연결을 표시합니다.
- **show system log buffer** —기본 syslog 정보를 표시합니다.
- **vpn trace dump** - VPN 프로세스에 대한 자세한 정보를 표시합니다.

```
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 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:
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto isakmp**(Cisco IOS Router) - IKE(Internet Key Exchange) 단계 I(Main Mode) 협상에 대한 자세한 정보를 표시합니다.
- **debug crypto ipsec**(Cisco IOS Router) - IKE phase II(Quick Mode) 협상에 대한 자세한 정보를 표시합니다.
- **debug crypto engine**(Cisco IOS Router) - 패킷 암호화/암호 해독 및 DH(Diffie-Hellman) 프로세스를 디버깅합니다.
- **debug ip rip**(Cisco IOS Router) - RIP 라우팅 프로토콜을 디버깅합니다.

VPN 5000 Concentrator에서 **show ip routing** 명령을 실행합니다.

```
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 FFFFFF00 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 FFFFFF00 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 FFFFFF00 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
```

관련 정보

- Cisco VPN 5000 Series Concentrator 지원 페이지
- Cisco VPN 5000 클라이언트 지원 페이지
- IPSec(IP Security Protocol) 지원 페이지
- Technical Support - Cisco Systems