Configuration de GRE sur IPSec entre un routeur Cisco IOS et un concentrateur VPN 5000 utilisant RIP et CVC

Contenu

Introduction

Cette configuration d'échantillon décrit comment configurer l'Encapsulation de routage générique (GRE) au-dessus d'IPSec entre un concentrateur de Cisco VPN 5000 et un routeur de Cisco IOS®. La fonction d'encapsulation GRE sous IPSec a été introduite dans la version 6.0(19) du logiciel du concentrateur VPN 5000.

Le Protocole RIP (Routing Information Protocol) est utilisé comme le protocole de routage dynamique dans cet échantillon pour conduire le trafic à travers le tunnel VPN.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS version 12.1(5)T7

- Version de logiciel de logiciel du concentrateur VPN 5000 6.0(19)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.

GRE au-dessus d'IPSec est configuré entre le routeur Cisco IOS (7140) et le Concentrateur Cisco VPN 5008. Derrière ces périphériques, de plusieurs réseaux sont annoncés par l'intermédiaire du RIP, qui fonctionne dans le tunnel GRE entre 7140 et VPN 5008.

Les réseaux derrière Cisco 7140 sont :

- 10.31.0.0/17

Les réseaux derrière le VPN 5008 sont :

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

Configurations

Ce document utilise les configurations indiquées ici.

- Routeur Cisco IOS
- Concentrateur VPN 5000
- CVC

Routeur Cisco IOS
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
```

Concentrateur VPN 5000

```
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#
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show ip route** — Affiche l'état actuel de la table de routage.
- **show crypto engine connection active** — Affiche le chiffrement des paquets/déchiffrement contre- par association de sécurité d'IPSec.
- **show crypto ipsec sa** — Affiche toutes les associations de sécurité en cours d'IPSec.
- **mémoire tampon de log de show system** — Affiche les informations de base de Syslog.
- **vidage mémoire de suivi de vpn** — Affiche les informations détaillées sur des processus 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 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:
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque: Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

- **debug crypto isakmp** (routeur Cisco IOS) — Affiche les informations détaillées sur la négociation de la phase I d'Échange de clés Internet (IKE) (mode principal).
- **debug crypto ipsec** (routeur Cisco IOS) — Affiche les informations détaillées sur la négociation de la phase II d'IKE (mode rapide).
- **debug crypto engine** (routeur Cisco IOS) — Débugge le chiffrement des paquets/déchiffrement et le processus de Protocole DH (Diffie-Hellman).
- **debug ip rip** (routeur Cisco IOS) — Débugge le protocole de routage de RIP.

Émettez le **show ip conduisant la** commande du concentrateur VPN 5000.

```
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
```

Informations connexes

- Page de support pour Concentrateurs VPN Cisco 5000
- Page d'assistance du client VPN 5000 de Cisco
- Page d'assistance d'IPSec (protocole de sécurité IP)
- Support technique - Cisco Systems