

Configuration de GRE et IPSec avec routage IPX

Contenu

[Introduction](#)

[Avant de commencer](#)

[Conditions préalables](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Exemple de sortie de show](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Exemple de sortie de débogage](#)

[Informations connexes](#)

Introduction

Ce document illustre une configuration IPSec (IP Security) à l'aide d'un tunnel GRE (Generic Routing Encapsulation) entre deux routeurs. IPSec peut être utilisé pour chiffrer les tunnels GRE afin de fournir une sécurité de couche réseau pour le trafic non IP, tel que Novell Internetwork Packet Exchange (IPX), AppleTalk, etc. Le tunnel GRE dans cet exemple est uniquement utilisé pour le transport de trafic non IP. Par conséquent, aucune adresse IP n'est configurée dans le tunnel. Voici quelques considérations de configuration :

- Avec le logiciel IOS 12.2(13)T et les versions ultérieures (logiciel T-train numéroté supérieur, 12.3 et ultérieures), la crypto-carte IPSec configurée doit uniquement être appliquée à l'interface physique et n'est plus nécessaire à l'application sur l'interface de tunnel GRE. Dans les versions logicielles antérieures à cette version, les crypto-cartes IPSec doivent être appliquées à l'interface du tunnel et à l'interface physique. La présence de la carte de chiffrement sur l'interface physique et de tunnel lors de l'utilisation du logiciel 12.2.(13)T et ultérieur doit continuer à fonctionner ; Cependant, Cisco vous recommande vivement de l'appliquer uniquement sur l'interface physique.
- Assurez-vous que le tunnel GRE fonctionne avant d'appliquer les crypto-cartes.
- La liste de contrôle d'accès de chiffrement (ACL) doit avoir GRE comme protocole autorisé. Par exemple, **access-list 101 permit gre host #.#.#.# host #.#.#.#.#** (où le premier numéro d'hôte est l'adresse IP de la source du tunnel du tunnel GRE et le second numéro d'hôte est l'adresse IP de la destination du tunnel).
- Utilisez les adresses IP de l'interface physique (ou de l'interface de bouclage) pour identifier les homologues IKE (Internet Key Exchange).

- Dans certaines versions antérieures de Cisco IOS, la commutation rapide sur l'interface de tunnel doit être désactivée pour qu'elle fonctionne, en raison d'un bogue. Désactivez la commutation rapide sur l'interface de tunnel. Vous pouvez afficher les détails du bogue pour ce problème sur [CSCdm10376](#) (clients [enregistrés](#) uniquement).

Avant de commencer

Conditions préalables

Avant d'essayer cette configuration, veuillez vous assurer que vous remplissez les conditions préalables suivantes :

- [connaissance de la configuration et du routage IPX](#)
- [connaissance et configuration des tunnels GRE](#)
- [connaissance de fonctionnement et configuration d'IPSec](#)

Components Used

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Logiciel Cisco IOS® Version 12.2(7)
- Routeurs de la gamme Cisco 3600

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

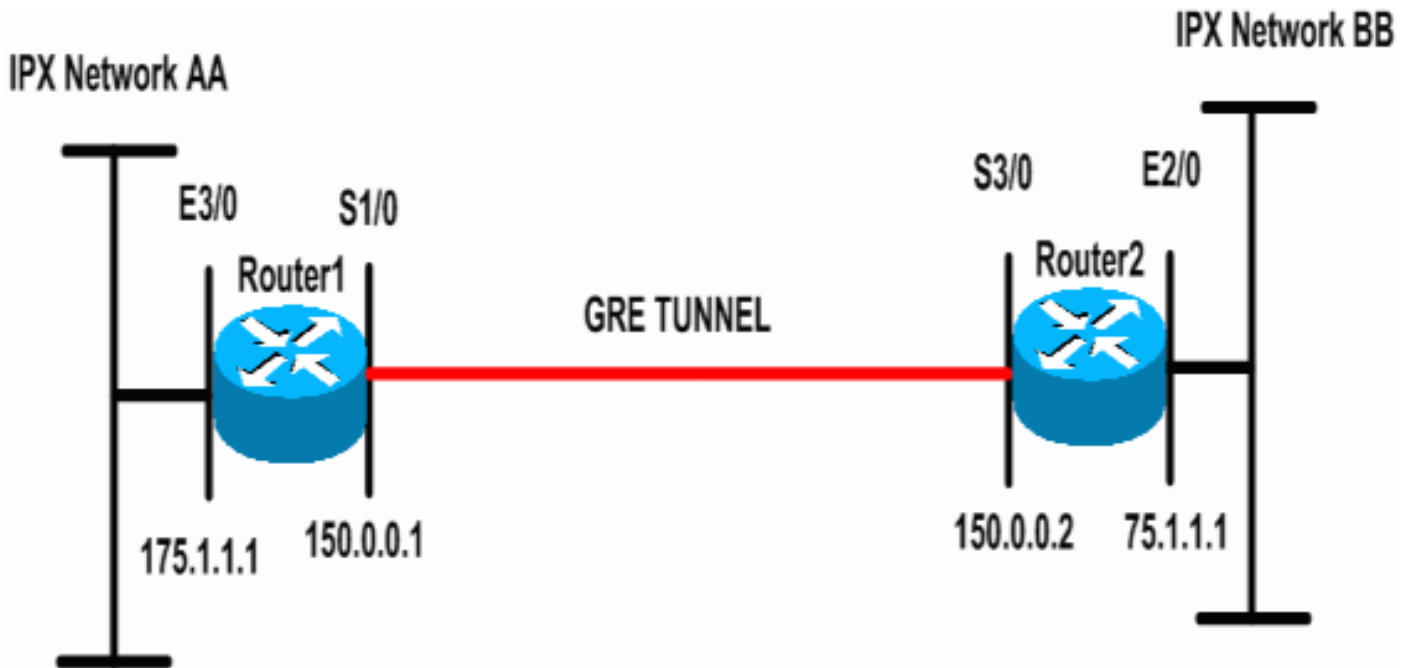
Configuration

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

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement).

Diagramme du réseau

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



[Configurations](#)

Ce document utilise les configurations présentées ci-dessous.

Routeur 1

```

Current configuration: 1300 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router1
!
ip subnet-zero
!
!--- Enables IPX routing. ipx routing 00e0.b064.258e
!
!--- Defines the IKE policy identifying the parameters
for building IKE SAs.
crypto isakmp policy 10
  authentication pre-share
  group 2
  lifetime 3600
!--- Defines the pre-shared key for the remote peer.
crypto isakmp key cisco address 200.1.1.1
!
!--- Defines the transform set to be used for IPSec SAs.
crypto ipsec transform-set tunnelset esp-des esp-md5-
hmac
!
!--- Configures the router to use the address of
Loopback0 interface !--- for IKE and IPSec traffic.
crypto map toBB local-address Loopback0
!--- Defines a crypto map to be used for establishing
IPSec SAs.
crypto map toBB 10 ipsec-isakmp
  set peer 200.1.1.1

```

```

set transform-set tunnelset
match address 101
!
interface Loopback0
 ip address 100.1.1.1 255.255.255.0
!
!--- Configures a GRE tunnel for transporting IPX
traffic. interface Tunnel0
no ip address

ipx network CC
tunnel source Serial1/0
tunnel destination 150.0.0.2

!
interface Serial1/0
 ip address 150.0.0.1 255.255.255.0
!--- Applies the crypto map to the physical interface
used !--- for carrying GRE tunnel traffic. crypto map
toBB
!
interface Ethernet3/0
 ip address 175.1.1.1 255.255.255.0
ipx network AA
!--- Output suppressed. ip classless ip route 0.0.0.0
0.0.0.0 150.0.0.2 no ip http server ! !--- Configures
GRE tunnel traffic to be encrypted using IPSec. access-
list 101 permit gre host 150.0.0.1 host 150.0.0.2
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end

```

Routeur 2

```

Current configuration:1525 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router2
!
ip subnet-zero
!
!--- Enables IPX routing. ipx routing 0010.7b37.c8ae
!
!--- Defines the IKE policy identifying the parameters
for building IKE SAs.
crypto isakmp policy 10
authentication pre-share
group 2
lifetime 3600
!--- Defines the pre-shared key for the remote peer.
crypto isakmp key cisco address 100.1.1.1
!
!--- Defines the transform set to be used for IPSec SAs.

```

```

crypto ipsec transform-set tunnelset esp-des esp-md5-
hmac
!
!--- Configures the router to use the address of
Loopback0 interface !--- for IKE and IPSec traffic.
crypto map toAA local-address Loopback0
!--- Defines a crypto map to be used for establishing
IPSec SAs.
crypto map toAA 10 ipsec-isakmp
  set peer 100.1.1.1
  set transform-set tunnelset
  match address 101
!
interface Loopback0
  ip address 200.1.1.1 255.255.255.0
!
!--- Configures a GRE tunnel for transporting IPX
traffic interface Tunnel0
no ip address

  ipx network CC
  tunnel source Serial3/0
  tunnel destination 150.0.0.1
!
interface Ethernet2/0
  ip address 75.1.1.1 255.255.255.0
  ipx network BB
!
interface Serial3/0
  ip address 150.0.0.2 255.255.255.0
  clockrate 9600
!--- Applies the crypto map to the physical interface
used !--- for carrying GRE tunnel traffic. crypto map
toAA
!
!--- Output suppressed. ip classless ip route 0.0.0.0
0.0.0.0 150.0.0.1 no ip http server ! !--- Configures
GRE tunnel traffic to be encrypted using IPSec. access-
list 101 permit gre host 150.0.0.2 host 150.0.0.1
!
line con 0
  transport input none
line aux 0
line vty 0 4
  login
!
end

```

Vérification

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 ipx interface](#) : affiche l'état et les paramètres des interfaces IPX configurées sur le périphérique, telles que le réseau IPX et l'adresse du noeud.
- [show ipx route](#) : affiche le contenu de la table de routage IPX.

- [show crypto isakmp sa](#) - Affiche les associations de sécurité de phase 1 en affichant l'association de sécurité IKE du routeur. L'état affiché doit être QM_IDLE pour qu'une SA IKE soit considérée comme active et opérationnelle.
- [show crypto ipsec sa](#) - Affiche les associations de sécurité de phase 2 en affichant une liste détaillée des SA IPSec actives du routeur.
- [show crypto map](#) - Affiche les crypto-cartes configurées sur le routeur, ainsi que ses détails tels que les listes d'accès de chiffrement, les jeux de transformation, les homologues, etc.
- [show crypto engine connections active](#) - Affiche une liste des SA actives avec leurs interfaces, transformations et compteurs associés.

Exemple de sortie de show

Cette section capture les sorties de la commande **show** sur le périphérique Router1 lorsque la commande **ping IPX** est exécutée sur Router1 destiné à Router2. Les sorties sur Router2 sont similaires. Les paramètres clés du résultat sont indiqués en **gras**. Pour obtenir des explications sur les sorties de commande, reportez-vous au document [IP Security Troubleshooting - Understanding and Using debug Commands](#).

```
Router1#show ipx interface ethernet 3/0
Ethernet3/0 is up, line protocol is up
  IPX address is AA.00b0.64cb.eab1, NOVELL-ETHER [up]
  Delay of this IPX network, in ticks is 1 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
!--- Output suppressed. Router2#show ipx interface ethernet 2/0
Ethernet2/0 is up, line protocol is up
  IPX address is BB.0002.16ae.c161, NOVELL-ETHER [up]
  Delay of this IPX network, in ticks is 1 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
!--- Output suppressed. Router1#show ipx route
Codes: C - Connected primary network,      c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses, U - Per-user static/Unknown, H - Hold-down

3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C          AA (NOVELL-ETHER),   Et3/0
C          CC (TUNNEL),        Tu0
R          BB [151/01] via      CC.0010.7b37.c8ae,   56s, Tu0

Router2#show ipx route
Codes: C - Connected primary network,      c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses, U - Per-user static/Unknown, H - Hold-down

3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C          BB (NOVELL-ETHER),   Et2/0
C          CC (TUNNEL),        Tu0
R          AA [151/01] via      CC.00e0.b064.258e,   8s, Tu0

Router1#ping ipx BB.0010.7b37.c8ae
```

Type escape sequence to abort.

Sending 5, 100-byte IPX Novell Echoes to BB.0002.16ae.c161, timeout is 2 seconds:
!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms

Router2#ping ipx AA.00b0.64cb.eab1

Type escape sequence to abort.

Sending 5, 100-byte IPX Novell Echoes to AA.00b0.64cb.eab1, timeout is 2 seconds:
!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms

Router1#show crypto isakmp sa

dst	src	state	conn-id	slot
200.1.1.1	100.1.1.1	QM_IDLE	5	0

Router1#show crypto ipsec sa detail

interface: Serial1/0

Crypto map tag: toBB, local addr. 100.1.1.1

local ident (addr/mask/prot/port): (150.0.0.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (150.0.0.2/255.255.255.255/47/0)

current_peer: 200.1.1.1

PERMIT, flags={origin_is_acl,}

#pkts encaps: 343, #pkts encrypt: 343, #pkts digest 343

#pkts decaps: 343, #pkts decrypt: 343, #pkts verify 343

#pkts compressed: 0, #pkts decompressed: 0

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

#pkts no sa (send) 1, #pkts invalid sa (rcv) 0

#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0

#pkts invalid prot (rcv) 0, #pkts verify failed: 0

#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0

#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0

##pkts replay failed (rcv): 0

#pkts internal err (send): 0, #pkts internal err (rcv) 0

local crypto endpt.: 100.1.1.1, remote crypto endpt.: 200.1.1.1

path mtu 1500, ip mtu 1500, ip mtu interface Serial1/0

current outbound spi: CB6F6DA6

inbound esp sas:

spi: 0xFD6F387(265745287)

transform: esp-des esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2010, flow_id: 11, crypto map: toBB

sa timing: remaining key lifetime (k/sec): (4607994/1892)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xCB6F6DA6(3413077414)

transform: esp-des esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2011, flow_id: 12, crypto map: toBB

sa timing: remaining key lifetime (k/sec): (4607994/1892)

IV size: 8 bytes

```
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
Router1#show crypto map
```

```
Crypto Map: "toBB" idb: Loopback0 local address: 100.1.1.1
```

```
Crypto Map "toBB" 10 ipsec-isakmp
```

```
Peer = 200.1.1.1
```

```
Extended IP access list 101
```

```
access-list 101 permit gre host 150.0.0.1 host 150.0.0.2
```

```
Current peer: 200.1.1.1
```

```
Security association lifetime: 4608000 kilobytes/3600 seconds
```

```
PFS (Y/N): N
```

```
Transform sets={ tunnelset, }
```

```
Interfaces using crypto map toBB:
```

```
Serial1/0
```

```
Router1#show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
5	<none>	<none>	set	HMAC_SHA+DES_56_CB	0	0
2010	Serial1/0	150.0.0.1	set	HMAC_MD5+DES_56_CB	0	40
2011	Serial1/0	150.0.0.1	set	HMAC_MD5+DES_56_CB	45	0

Dépannage

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

Dépannage des commandes

Note : Avant d'émettre des commandes **debug**, consultez [Informations importantes sur les commandes de débogage](#).

- [debug crypto engine](#) - Affiche des informations sur le moteur de chiffrement qui effectue le chiffrement et le déchiffrement.
- [debug crypto ipsec](#) - Affichez les négociations IPsec de la phase 2.
- [debug crypto isakmp](#) - Affichez les négociations IKE de la phase 1.

Exemple de sortie de débogage

Cette section capture les sorties de la commande debug sur les routeurs configurés avec IPsec. La commande **ping** IPX est exécutée sur le routeur 1 destiné au routeur 2.

- [Routeur 1](#)
- [Routeur 2](#)

Routeur 1

Router1#show debug

Cryptographic Subsystem:

Crypto ISAKMP debugging is on

Crypto Engine debugging is on

Crypto IPSEC debugging is on

Router1#

!--- GRE traffic matching crypto ACL triggers IPsec processing *Mar 2 00:41:17.593:

IPSEC(sa_request): ,

(key eng. msg.) OUTBOUND local= 100.1.1.1, remote= 200.1.1.1,

local_proxy= 150.0.0.1/255.255.255.255/47/0 (type=1),

remote_proxy= 150.0.0.2/255.255.255.255/47/0 (type=1),

protocol= ESP, transform= esp-des esp-md5-hmac ,

lifedur= 3600s and 4608000kb,

spi= 0x9AAD0079(2595029113), conn_id= 0, keysize= 0, flags= 0x400C

*Mar 2 00:41:17.597: ISAKMP: received ke message (1/1)

!--- IKE uses UDP port 500, begins main mode exchange. *Mar 2 00:41:17.597: ISAKMP: local port 500, remote port 500

*Mar 2 00:41:17.597: ISAKMP (0:1): beginning Main Mode exchange

*Mar 2 00:41:17.597: ISAKMP (0:1): sending packet to 200.1.1.1 (I) MM_NO_STATE

*Mar 2 00:41:17.773: ISAKMP (0:1): received packet from 200.1.1.1 (I) MM_NO_STATE

*Mar 2 00:41:17.773: ISAKMP (0:1): processing SA payload. message ID = 0

*Mar 2 00:41:17.773: ISAKMP (0:1): found peer pre-shared key matching 200.1.1.1

*Mar 2 00:41:17.773: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 10 policy

!--- IKE SAs are negotiated. *Mar 2 00:41:17.773: ISAKMP: encryption DES-CBC

*Mar 2 00:41:17.773: ISAKMP: hash SHA

*Mar 2 00:41:17.773: ISAKMP: default group 2

*Mar 2 00:41:17.773: ISAKMP: auth pre-share

*Mar 2 00:41:17.773: ISAKMP: life type in seconds

*Mar 2 00:41:17.773: ISAKMP: life duration (basic) of 3600

*Mar 2 00:41:17.773: ISAKMP (0:1): atts are acceptable. Next payload is 0

*Mar 2 00:41:17.773: CryptoEngine0: generate alg parameter

*Mar 2 00:41:17.905: CRYPTO_ENGINE: Dh phase 1 status: 0

*Mar 2 00:41:17.905: CRYPTO_ENGINE: Dh phase 1 status: 0

*Mar 2 00:41:17.905: ISAKMP (0:1): SA is doing pre-shared key authentication using id type

ID_IPV4_

ADDR

*Mar 2 00:41:17.905: ISAKMP (0:1): sending packet to 200.1.1.1 (I) MM_SA_SETUP

*Mar 2 00:41:18.149: ISAKMP (0:1): received packet from 200.1.1.1 (I) MM_SA_SETUP

*Mar 2 00:41:18.153: ISAKMP (0:1): processing KE payload. message ID = 0

*Mar 2 00:41:18.153: CryptoEngine0: generate alg parameter

*Mar 2 00:41:18.317: ISAKMP (0:1): processing NONCE payload. message ID = 0

*Mar 2 00:41:18.317: ISAKMP (0:1): found peer pre-shared key matching 200.1.1.1

*Mar 2 00:41:18.317: CryptoEngine0: create ISAKMP SKEYID for conn id 1

*Mar 2 00:41:18.321: ISAKMP (0:1): SKEYID state generated

*Mar 2 00:41:18.321: ISAKMP (0:1): processing vendor id payload

*Mar 2 00:41:18.321: ISAKMP (0:1): speaking to another IOS box!

*Mar 2 00:41:18.321: ISAKMP (1): ID payload

next-payload : 8

type : 1

protocol : 17

port : 500

length : 8

*Mar 2 00:41:18.321: ISAKMP (1): Total payload length: 12

*Mar 2 00:41:18.321: CryptoEngine0: generate hmac context for conn id 1

*Mar 2 00:41:18.321: ISAKMP (0:1): sending packet to 200.1.1.1 (I) MM_KEY_EXCH

*Mar 2 00:41:18.361: ISAKMP (0:1): received packet from 200.1.1.1 (I) MM_KEY_EXCH

*Mar 2 00:41:18.361: ISAKMP (0:1): processing ID payload. message ID = 0

*Mar 2 00:41:18.361: ISAKMP (0:1): processing HASH payload. message ID = 0

*Mar 2 00:41:18.361: CryptoEngine0: generate hmac context for conn id 1

!--- Peer is authenticated. *Mar 2 00:41:18.361: ISAKMP (0:1): SA has been authenticated with

200.1.1.1

!--- Begins quick mode exchange. *Mar 2 00:41:18.361: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of -2078851837

*Mar 2 00:41:18.365: CryptoEngine0: generate hmac context for conn id 1
*Mar 2 00:41:18.365: ISAKMP (0:1): sending packet to 200.1.1.1 (I) QM_IDLE
*Mar 2 00:41:18.365: CryptoEngine0: clear dh number for conn id 1
*Mar 2 00:41:18.681: ISAKMP (0:1): received packet from 200.1.1.1 (I) QM_IDLE
*Mar 2 00:41:18.681: CryptoEngine0: generate hmac context for conn id 1
*Mar 2 00:41:18.685: ISAKMP (0:1): processing HASH payload. message ID = -2078851837
*Mar 2 00:41:18.685: ISAKMP (0:1): processing SA payload. message ID = -2078851837

!--- Negotiates IPsec SA. *Mar 2 00:41:18.685: ISAKMP (0:1): Checking IPsec proposal 1

*Mar 2 00:41:18.685: ISAKMP: transform 1, ESP_DES
*Mar 2 00:41:18.685: ISAKMP: attributes in transform:
*Mar 2 00:41:18.685: ISAKMP: encaps is 1
*Mar 2 00:41:18.685: ISAKMP: SA life type in seconds
*Mar 2 00:41:18.685: ISAKMP: SA life duration (basic) of 3600
*Mar 2 00:41:18.685: ISAKMP: SA life type in kilobytes
*Mar 2 00:41:18.685: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Mar 2 00:41:18.685: ISAKMP: authenticator is HMAC-MD5
*Mar 2 00:41:18.685: validate proposal 0
*Mar 2 00:41:18.685: ISAKMP (0:1): atts are acceptable.

*Mar 2 00:41:18.685: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 100.1.1.1, remote= 200.1.1.1,
local_proxy= 150.0.0.1/255.255.255.255/47/0 (type=1),
remote_proxy= 150.0.0.2/255.255.255.255/47/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

*Mar 2 00:41:18.689: validate proposal request 0
*Mar 2 00:41:18.689: ISAKMP (0:1): processing NONCE payload. message ID = -2078851837
*Mar 2 00:41:18.689: ISAKMP (0:1): processing ID payload. message ID = -2078851837
*Mar 2 00:41:18.689: ISAKMP (0:1): processing ID payload. message ID = -2078851837
*Mar 2 00:41:18.689: CryptoEngine0: generate hmac context for conn id 1
*Mar 2 00:41:18.689: ipsec allocate flow 0
*Mar 2 00:41:18.689: ipsec allocate flow 0

!--- IPsec SAs are generated for inbound and outbound traffic. *Mar 2 00:41:18.693: ISAKMP (0:1): Creating IPsec SAs

*Mar 2 00:41:18.693: inbound SA from 200.1.1.1 to 100.1.1.1
(proxy 150.0.0.2 to 150.0.0.1)
*Mar 2 00:41:18.693: has spi 0x9AAD0079 and conn_id 2000 and flags 4
*Mar 2 00:41:18.693: lifetime of 3600 seconds
*Mar 2 00:41:18.693: lifetime of 4608000 kilobytes
*Mar 2 00:41:18.693: outbound SA from 100.1.1.1 to 200.1.1.1 (proxy
150.0.0.1
to 150.0.0.2)

*Mar 2 00:41:18.693: has spi -1609905338 and conn_id 2001 and flags C
*Mar 2 00:41:18.693: lifetime of 3600 seconds
*Mar 2 00:41:18.693: lifetime of 4608000 kilobytes
*Mar 2 00:41:18.697: ISAKMP (0:1): sending packet to 200.1.1.1 (I) QM_IDLE
*Mar 2 00:41:18.697: ISAKMP (0:1): deleting node -2078851837 error FALSE reason "
*Mar 2 00:41:18.697: IPSEC(key_engine): got a queue event...
*Mar 2 00:41:18.697: IPSEC(initialize_sas): ,

(key eng. msg.) INBOUND local= 100.1.1.1, remote= 200.1.1.1,
local_proxy= 150.0.0.1/0.0.0.0/47/0 (type=1),
remote_proxy= 150.0.0.2/0.0.0.0/47/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x9AAD0079(2595029113), conn_id= 2000, keysize= 0, flags= 0x4

*Mar 2 00:41:18.697: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 100.1.1.1, remote= 200.1.1.1,
local_proxy= 150.0.0.1/0.0.0.0/47/0 (type=1),
remote_proxy= 150.0.0.2/0.0.0.0/47/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,

```
spi= 0xA00ACB46(2685061958), conn_id= 2001, keysize= 0, flags= 0xC
*Mar 2 00:41:18.697: IPSEC(create_sa): sa created,
(sa) sa_dest= 100.1.1.1, sa_prot= 50,
sa_spi= 0x9AAD0079(2595029113),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
*Mar 2 00:41:18.701: IPSEC(create_sa): sa created,
(sa) sa_dest= 200.1.1.1, sa_prot= 50,
sa_spi= 0xA00ACB46(2685061958),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
```

Router1#

Routeur 2

Router2#**show debug**

Cryptographic Subsystem:

```
Crypto ISAKMP debugging is on
Crypto Engine debugging is on
Crypto IPSEC debugging is on
```

Router2#

```
!--- IKE processing begins here. *Mar 2 00:30:26.093: ISAKMP (0:0): received packet from
100.1.1.1 (N) NEW SA
*Mar 2 00:30:26.093: ISAKMP: local port 500, remote port 500
*Mar 2 00:30:26.093: ISAKMP (0:1): processing SA payload. message ID = 0
*Mar 2 00:30:26.093: ISAKMP (0:1): found peer pre-shared key matching 100.1.1.1
!--- IKE SAs are negotiated. *Mar 2 00:30:26.093: ISAKMP (0:1): Checking ISAKMP transform 1
against priority 10 policy
*Mar 2 00:30:26.093: ISAKMP: encryption DES-CBC
*Mar 2 00:30:26.093: ISAKMP: hash SHA
*Mar 2 00:30:26.093: ISAKMP: default group 2
*Mar 2 00:30:26.093: ISAKMP: auth pre-share
*Mar 2 00:30:26.093: ISAKMP: life type in seconds
*Mar 2 00:30:26.093: ISAKMP: life duration (basic) of 3600
*Mar 2 00:30:26.093: ISAKMP (0:1): atts are acceptable. Next payload is 0
*Mar 2 00:30:26.097: CryptoEngine0: generate alg parameter
*Mar 2 00:30:26.229: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar 2 00:30:26.229: CRYPTO_ENGINE: Dh phase 1 status: 0
*Mar 2 00:30:26.229: ISAKMP (0:1): SA is doing pre-shared key authentication using id type
ID_IPV4_
ADDR
*Mar 2 00:30:26.229: ISAKMP (0:1): sending packet to 100.1.1.1 (R) MM_SA_SETUP
*Mar 2 00:30:26.417: ISAKMP (0:1): received packet from 100.1.1.1 (R) MM_SA_SETUP
*Mar 2 00:30:26.417: ISAKMP (0:1): processing KE payload. message ID = 0
*Mar 2 00:30:26.417: CryptoEngine0: generate alg parameter
*Mar 2 00:30:26.589: ISAKMP (0:1): processing NONCE payload. message ID = 0
*Mar 2 00:30:26.589: ISAKMP (0:1): found peer pre-shared key matching 100.1.1.1
*Mar 2 00:30:26.593: CryptoEngine0: create ISAKMP SKEYID for conn id 1
*Mar 2 00:30:26.593: ISAKMP (0:1):
SKEYID state generated
*Mar 2 00:30:26.593: ISAKMP (0:1): processing vendor id payload
*Mar 2 00:30:26.593: ISAKMP (0:1): speaking to another IOS box!
*Mar 2 00:30:26.593: ISAKMP (0:1): sending packet to 100.1.1.1 (R) MM_KEY_EXCH
*Mar 2 00:30:26.813: ISAKMP (0:1): received packet from 100.1.1.1 (R) MM_KEY_EXCH
*Mar 2 00:30:26.817: ISAKMP (0:1): processing ID payload. message ID = 0
*Mar 2 00:30:26.817: ISAKMP (0:1): processing HASH payload. message ID = 0
*Mar 2 00:30:26.817: CryptoEngine0: generate hmac context for conn id 1
!--- Peer is authenticated. *Mar 2 00:30:26.817: ISAKMP (0:1): SA has been authenticated with
100.1.1.1
*Mar 2 00:30:26.817: ISAKMP (1): ID payload
next-payload : 8
```

```

type          : 1
protocol      : 17
port         : 500
length       : 8
*Mar 2 00:30:26.817: ISAKMP (1): Total payload length: 12
*Mar 2 00:30:26.817: CryptoEngine0: generate hmac context for conn id 1
*Mar 2 00:30:26.817: CryptoEngine0: clear dh number for conn id 1
*Mar 2 00:30:26.821: ISAKMP (0:1): sending packet to 100.1.1.1 (R) QM_IDLE
*Mar 2 00:30:26.869: ISAKMP (0:1): received packet from 100.1.1.1 (R) QM_IDLE
*Mar 2 00:30:26.869: CryptoEngine0: generate hmac context for conn id 1
*Mar 2 00:30:26.869: ISAKMP (0:1): processing HASH payload. message ID = -2078851837
*Mar 2 00:30:26.873: ISAKMP (0:1): processing SA payload. message ID = -2078851837
!--- IPsec SAs are negotiated. *Mar 2 00:30:26.873: ISAKMP (0:1): Checking IPsec proposal 1
*Mar 2 00:30:26.873: ISAKMP: transform 1, ESP_DES
*Mar 2 00:30:26.873: ISAKMP:   attributes in transform:
*Mar 2 00:30:26.873: ISAKMP:     encaps is 1
*Mar 2 00:30:26.873: ISAKMP:     SA life type in seconds
*Mar 2 00:30:26.873: ISAKMP:     SA life duration (basic) of 3600
*Mar 2 00:30:26.873: ISAKMP:     SA life type in kilobytes
*Mar 2 00:30:26.873: ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Mar 2 00:30:26.873: ISAKMP:     authenticator is HMAC-MD5
*Mar 2 00:30:26.873: validate proposal 0
*Mar 2 00:30:26.873: ISAKMP (0:1): atts are acceptable.
*Mar 2 00:30:26.873: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 200.1.1.1, remote= 100.1.1.1,
local_proxy= 150.0.0.2/255.255.255.255/47/0 (type=1),
remote_proxy= 150.0.0.1/255.255.255.255/47/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar 2 00:30:26.873: validate proposal request 0
*Mar 2 00:30:26.877: ISAKMP (0:1): processing NONCE payload. message ID = -2078851837
*Mar 2 00:30:26.877: ISAKMP (0:1): processing ID payload. message ID = -2078851837
*Mar 2 00:30:26.877: ISAKMP (0:1): processing ID payload. message ID = -2078851837
*Mar 2 00:30:26.877: ISAKMP (0:1): asking for 1 spis from ipsec
*Mar 2 00:30:26.877: IPSEC(key_engine): got a queue event...
*Mar 2 00:30:26.877: IPSEC(spi_response): getting spi 2685061958 for SA
from 200.1.1.1 to 100.1.1.1 for prot 3
*Mar 2 00:30:26.877: ISAKMP: received ke message (2/1)
*Mar 2 00:30:27.129: CryptoEngine0: generate hmac context for conn id 1
*Mar 2 00:30:27.129: ISAKMP (0:1): sending packet to 100.1.1.1 (R) QM_IDLE
*Mar 2 00:30:27.185: ISAKMP (0:1): received packet from 100.1.1.1 (R) QM_IDLE
*Mar 2 00:30:27.189: CryptoEngine0: generate hmac context for conn id 1
*Mar 2 00:30:27.189: ipsec allocate flow 0
*Mar 2 00:30:27.189: ipsec allocate flow 0
!--- IPsec SAs are generated for inbound and outbound traffic. *Mar 2 00:30:27.193: ISAKMP
(0:1): Creating IPsec SAs
*Mar 2 00:30:27.193:   inbound SA from 100.1.1.1 to 200.1.1.1
(proxy 150.0.0.1 to 150.0.0.2)
*Mar 2 00:30:27.193:   has spi 0xA00ACB46 and conn_id 2000 and flags 4
*Mar 2 00:30:27.193:   lifetime of 3600 seconds
*Mar 2 00:30:27.193:   lifetime of 4608000 kilobytes
*Mar 2 00:30:27.193:   outbound SA from 200.1.1.1 to 100.1.1.1 (proxy
150.0.0.2
to 150.0.0.1 )
*Mar 2 00:30:27.193:   has spi -1699938183 and conn_id 2001 and flags C
*Mar 2 00:30:27.193:   lifetime of 3600 seconds
*Mar 2 00:30:27.193:   lifetime of 4608000 kilobytes
*Mar 2 00:30:27.193: ISAKMP (0:1): deleting node -2078851837 error FALSE reason "quick mode
done (a
wait() "
*Mar 2 00:30:27.193: IPSEC(key_engine): got a queue event...
*Mar 2 00:30:27.193: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 200.1.1.1, remote= 100.1.1.1,

```

```
local_proxy= 150.0.0.2/0.0.0.0/47/0 (type=1),
remote_proxy= 150.0.0.1/0.0.0.0/47/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xA00ACB46(2685061958), conn_id= 2000, keysize= 0, flags= 0x4
*Mar  2 00:30:27.197: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 200.1.1.1, remote= 100.1.1.1,
local_proxy= 150.0.0.2/0.0.0.0/47/0 (type=1),
remote_proxy= 150.0.0.1/0.0.0.0/47/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x9AAD0079(2595029113), conn_id= 2001, keysize= 0, flags= 0xC
*Mar  2 00:30:27.197: IPSEC(create_sa): sa created,
(sa) sa_dest= 200.1.1.1, sa_prot= 50,
sa_spi= 0xA00ACB46(2685061958),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
*Mar  2 00:30:27.197: IPSEC(create_sa): sa created,
(sa) sa_dest= 100.1.1.1, sa_prot= 50,
sa_spi= 0x9AAD0079(2595029113),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
```

Router2#

[Informations connexes](#)

- [Page d'assistance technologique GRE](#)
- [Page d'assistance technique sur la sécurité IP \(IPSec\)](#)
- [Support technique - Cisco Systems](#)