

Configuration d'IPSec sur ADSL sur Cisco 2600/3600 avec ADSL-WIC et modules de chiffrement matériel

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Cavates](#)

[Vérification](#)

[Dépannage](#)

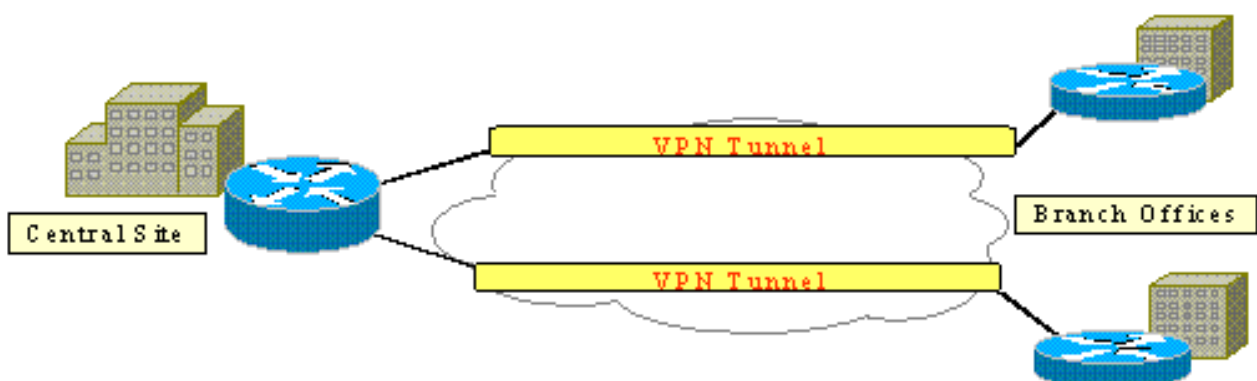
[Dépannage des commandes](#)

[Résumé](#)

[Informations connexes](#)

Introduction

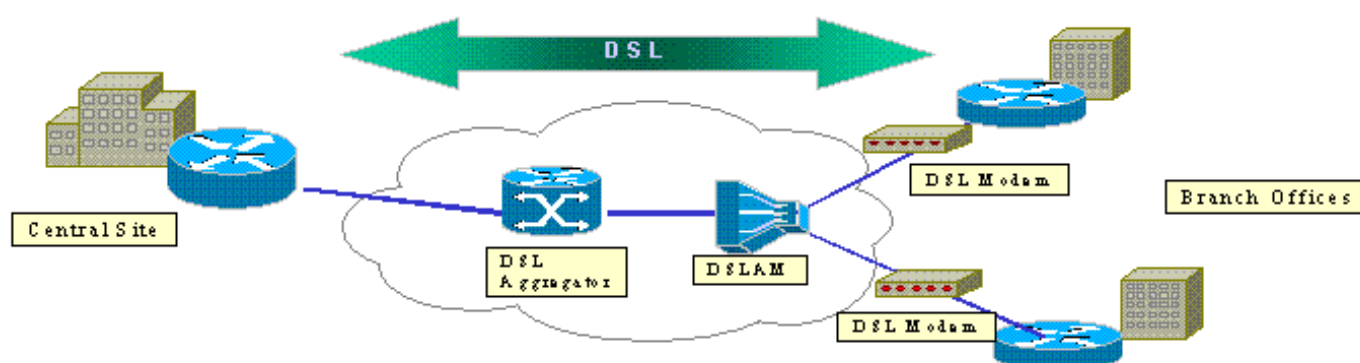
À mesure que l'Internet se développe, les filiales exigent que leurs connexions aux sites centraux soient à la fois fiables et sécurisées. Les réseaux privés virtuels (VPN) protègent les informations entre les bureaux distants et les sites centraux lorsqu'elles circulent sur Internet. La sécurité IP (IPSec) peut être utilisée pour garantir que les données qui traversent ces VPN sont cryptées. Le chiffrement fournit une autre couche de sécurité réseau.



Cette figure illustre un VPN IPSec type. Un certain nombre de connexions d'accès à distance et

de site à site sont impliquées entre les filiales et les sites centraux. En règle générale, les liaisons WAN traditionnelles telles que Frame Relay, RNIS et la connexion commutée par modem sont provisionnées entre les sites. Ces connexions peuvent impliquer des frais de provisionnement uniques et des frais mensuels élevés. En outre, pour les utilisateurs RNIS et modem, les temps de connexion peuvent être longs.

La ligne ADSL (Asymmetric Digital Subscriber Line) offre une alternative permanente et économique à ces liaisons WAN traditionnelles. Les données cryptées IPSec sur une liaison ADSL offrent une connexion sécurisée et fiable et permettent aux clients d'économiser de l'argent. Un équipement client ADSL traditionnel (CPE) configuré dans une succursale nécessite un modem ADSL qui se connecte à un périphérique qui émet et termine le trafic IPSec. Cette figure illustre un réseau ADSL classique.



Les routeurs Cisco 2600 et 3600 prennent en charge la carte d'interface WAN ADSL (WIC-1ADSL). Cette WIC-1ADSL est une solution d'accès à distance multiservice conçue pour répondre aux besoins d'une filiale. L'introduction des modules WIC-1ADSL et de cryptage matériel répond à la demande en IPSec et DSL dans une filiale dans une solution de routeur unique. Le WIC-1ADSL élimine la nécessité d'un modem DSL distinct. Le module de cryptage matériel fournit jusqu'à dix fois les performances par rapport au cryptage logiciel uniquement, car il décharge le cryptage qui traite à partir du routeur.

Pour plus d'informations sur ces deux produits, reportez-vous à [Cartes d'interface WAN ADSL pour les routeurs d'accès modulaire](#) et [les modules de réseau privé virtuel des gammes Cisco 1700, 2600, 3600 et 3700](#). Série.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

Routeurs de la gamme Cisco 2600/3600 :

- Logiciel Cisco IOS® Version 12.1(5)YB Enterprise PLUS 3DES

- DRAM : 64 Mo pour la gamme Cisco 2600, DRAM : 96 Mo pour la gamme Cisco 3600
- Flash 16 Mo pour la gamme Cisco 2600, Flash 32 Mo pour la gamme Cisco 3600
- ADSL WIC-1
- Modules de chiffrement matériel AIM-VPN/BP et AIM-VPN/EP pour la gamme Cisco 2600NM-VPN/MP pour Cisco 3620/3640 AIM-VPN/HP pour le Cisco 3660

Gamme Cisco 6400 :

- Logiciel Cisco IOS Version 12.1(5)DC1
- DRAM : 64 Mo
- Flash 8 Mo

Gamme Cisco 6160 :

- Logiciel Cisco IOS Version 12.1(7)DA2
- DRAM : 64 Mo
- Flash 16 Mo

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

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

Configuration

Cette section présente les informations que vous pouvez utiliser pour configurer les fonctionnalités décrites dans ce document.

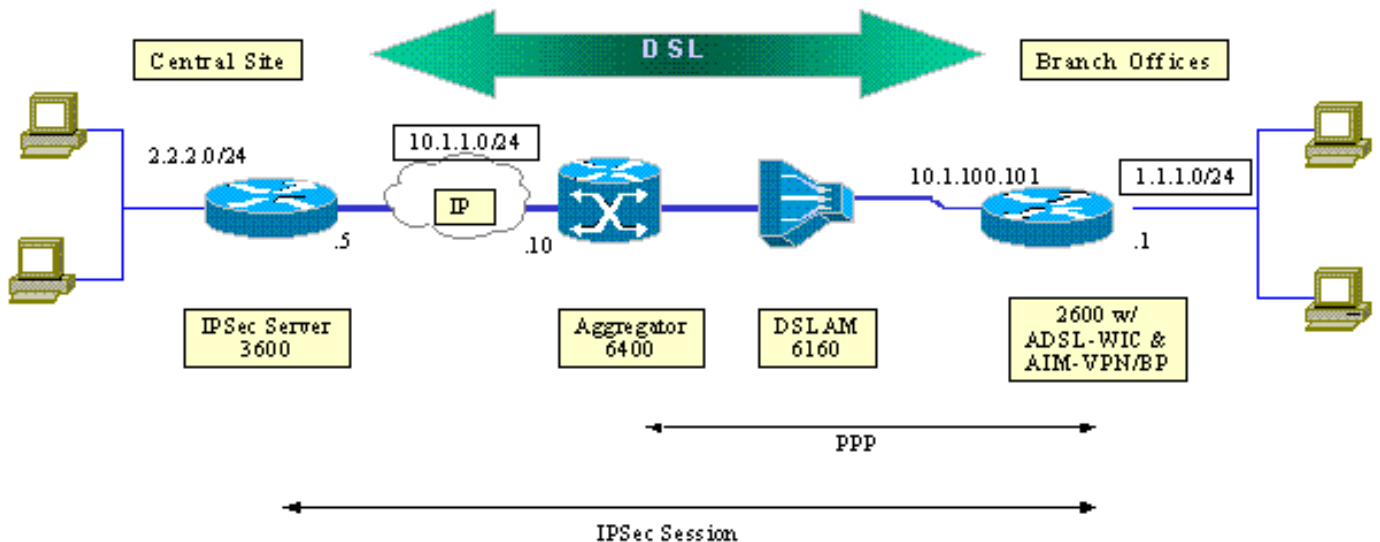
Remarque : Afin de trouver des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'[Outil de recherche de commandes](#) (clients [enregistrés](#) uniquement).

Diagramme du réseau

Ce document utilise la configuration réseau illustrée dans ce schéma.

Ce test simule une connexion VPN IPSec qui utilise l'ADSL dans un environnement de filiale classique.

Le Cisco 2600/3600 avec la carte d'interface WAN ADSL et le module de cryptage matériel assure la liaison avec un multiplexeur d'accès DSLAM (Digital Subscriber Line Access Multiplexer) Cisco 6160. Le Cisco 6400 est utilisé comme périphérique d'agrégation qui met fin à une session PPP qui démarre à partir du routeur Cisco 2600. Le tunnel IPSec provient du CPE 2600 et se termine au Cisco 3600 dans le bureau central, le périphérique de tête de réseau IPSec dans ce scénario. Le périphérique de tête de réseau est configuré pour accepter les connexions de n'importe quel client au lieu de l'appariement individuel. Le périphérique de tête de réseau est également testé avec uniquement des clés pré-partagées et le code HMAC (Message Authentication Code) basé sur le hachage 3DES et ESP (Edge Service Processor)-SHA (Secure Hash Algorithm).



Configurations

Ce document utilise les configurations suivantes :

- [Routeur Cisco 2600](#)
- [Périphérique de tête de réseau IPsec - Routeur Cisco 3600](#)
- [DSLAM Cisco 6160](#)
- [Processeur de routage de noeud Cisco 6400 \(NRP\)](#)

Notez ces points sur les configurations :

- Une clé pré-partagée est utilisée. Pour configurer des sessions IPsec sur plusieurs homologues, vous devez définir plusieurs instructions de définition de clé ou configurer une crypto-carte dynamique. Si toutes les sessions partagent une seule clé, vous devez utiliser une adresse homologue de 0.0.0.0.
- Le jeu de transformation peut être défini pour ESP, Authentication Header (AH) ou les deux pour une double authentification.
- Au moins une définition de stratégie de chiffrement doit être définie par homologue. Les crypto-cartes décident de l'homologue à utiliser pour créer la session IPsec. La décision est basée sur la correspondance d'adresses définie dans la liste de contrôle d'accès. Dans ce cas, il s'agit de la liste d'accès 101.
- Les crypto-cartes doivent être définies pour les interfaces physiques (interface ATM 0/0 dans ce cas) et le modèle virtuel.
- La configuration présentée dans ce document traite uniquement d'un tunnel IPsec sur une connexion DSL. Des fonctions de sécurité supplémentaires sont probablement nécessaires pour garantir que votre réseau n'est pas vulnérable. Ces fonctions de sécurité peuvent inclure des listes de contrôle d'accès (ACL) supplémentaires, la traduction d'adresses réseau (NAT) et l'utilisation d'un pare-feu avec une unité externe ou un jeu de fonctions de pare-feu IOS. Chacune de ces fonctions peut être utilisée afin de limiter le trafic non IPsec à destination et en provenance du routeur.

Routeur Cisco 2600

```

crypto isakmp policy 10
!--- Defines the ISAKMP parameters to be negotiated.
authentication pre-share !--- Defines the pre-shared key
to be exchanged with the peer. crypto isakmp key pre-
shared address 10.1.1.5 ! crypto ipsec transform-set
strong esp-des esp-sha-hmac !--- Defines the transform
set for ESP and/or AH. ! crypto map vpn 10 ipsec-isakmp
set peer 10.1.1.5 set transform-set strong match address
102 !--- Defines the crypto policy that includes the
peer IP address, !--- transform set that is used, as
well as the access list !--- that defines the packets
that are encrypted. ! interface ATM0/0 no ip address atm
vc-per-vp 256 no atm ilmi-keepalive dsl operating-mode
auto no fair-queue ! interface ATM0/0.1 point-to-point
pvc 0/35 encapsulation aal5mux ppp dialer dialer pool-
member 1 ! crypto map vpn !--- Applies the crypto map to
the ATM sub-interface. ! interface FastEthernet0/1 ip
address 1.1.1.1 255.255.255.0 duplex 100 speed full !
interface Dialer1 ip address 10.1.100.101 255.255.255.0
dialer pool 1 encapsulation ppp ppp pap sent-username
2621a password 7 045802150C2E crypto map vpn !---
Applies the crypto map to the Dialer interface. ! ip
classless ! ip route 2.2.2.0 255.255.255.0 10.1.1.5 ip
route 10.1.1.0 255.255.255.0 10.1.100.1 !--- Static
routes between 2600 CPE and IPSec server. ip route
0.0.0.0 0.0.0.0 Dialer1 ! access-list 102 permit ip
1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255 !--- Access list
that defines the addresses that are encrypted. ! end

```

Périphérique de tête de réseau IPSec - Routeur Cisco 3600

```

crypto isakmp policy 10
!--- Defines the ISAKMP parameters to be negotiated.
authentication pre-share !--- Defines the pre-shared key
to be exchanged with the peer. crypto isakmp key pre-
shared address 10.1.100.101 ! crypto ipsec transform-set
strong esp-des esp-sha-hmac !--- Defines the transform
set for ESP and/or AH. ! crypto map vpn 10 ipsec-isakmp
set peer 10.1.100.101 set transform-set strong match
address 102 !--- Defines the crypto policy that includes
the peer IP address, !--- transform set that are used,
and the access list !--- that defines the packets to be
encrypted. ! interface FastEthernet0/0 ip address
10.1.1.5 255.255.255.0 duplex 100 speed full crypto map
vpn !--- Applies the crypto map to the Fast Ethernet
interface. ! interface FastEthernet0/1 ip address
2.2.2.1 255.255.255.0 speed full full-duplex ! ip route
1.1.1.0 255.255.255.0 10.1.1.10 ip route 10.1.100.0
255.255.255.0 10.1.1.10 ! access-list 102 permit ip
2.2.2.0 0.0.0.255 1.1.1.0 0.0.0.255 !--- Access list
that defines the addresses to be encrypted. ! end

```

DSLAM Cisco 6160

```

dsl-profile full
dmt bitrate maximum fast downstream 10240 upstream 1024
dmt bitrate maximum interleaved downstream 0 upstream 0
!
atm address
47.0091.8100.0000.0004.6dd6.7c01.0004.6dd6.7c01.00
atm router pnni
no aesa embedded-number left-justified

```

```

none 1 level 56 lowest
redistribute atm-static
!
interface atm0/0
no ip address
atm maxvp-number 0
atm maxvc-number 4096
atm maxvci-bits 12
!
interface atm 1/2
no ip address
dsl profile full
no atm ilmi-keepalive
atm soft-vc 0 35 dest-address
47.0091.8100.0000.0004.c12b.cd81.4000.0c80.8000.00 0 36
rx-cttr 1 tx-cttr 1
!--- The previous two lines need to be on one line. !---
The network service access point (NSAP) !--- address
comes from the NSP on the Cisco 6400. Issue !--- a show
atm address command.

!

```

NRP Cisco 6400

```

!
username cisco password cisco
!
vc-class atm pppoa
encapsulation aal5mux ppp Virtual-templatel
!
interface loopback 0
ip address 10.1.100.1 255.255.255.0
!
interface atm 0/0/0
no ip address
no ip route-cache
no ip mroute-cache
no atm auto-configuration
atm ilmi-keepalive 10
pvc 0/16 ilmi
!
hold-queue 1000 in
!
interface atm 0/0/0.1 multipoint
no ip route-cache
no ip mroute-cach
class-int pppoa
pvc 0/36
!
interface fast 0/0/0
ip address 10.1.1.10 255.255.255.0
no ip route-cache
no ip mroute-cache
half-duplex
!
interface Virtual-Templatel
ip unnumbered Loopback0
no ip route-cache
peer default ip address pool pppoa
ppp authentication pap chap
ppp ipcp accept-address
ppp multilink

```

```
no ppp multilink fragmentation
!
ip local pool pppoa 10.1.100.2 10.1.100.100
!
```

Cavates

Les connexions ADSL peuvent être configurées avec un modèle virtuel ou une interface de numérotation.

Une interface de numérotation est utilisée afin de configurer le CPE DSL pour recevoir une adresse du fournisseur de services (l'adresse IP est négociée). Une interface de modèle virtuel est une interface descendante et ne prend pas en charge l'option d'adresse négociée, qui est nécessaire dans l'environnement DSL. Les interfaces de modèles virtuels ont été initialement mises en oeuvre pour les environnements DSL. Actuellement, une interface de numérotation est la configuration recommandée côté DSL CPE.

Deux problèmes sont détectés au moment de la configuration des interfaces de numérotation avec IPSec :

- ID de bogue Cisco [CSCdu30070](#) (clients [enregistrés](#) uniquement) —IPSec logiciel uniquement sur DSL : coin de file d'attente d'entrée sur l'interface de numérotation DSL.
- ID de bogue Cisco [CSCdu30335](#) (clients [enregistrés](#) uniquement) —IPSec matériel sur DSL : coin file d'attente d'entrée sur l'interface de numérotation.

La solution de contournement actuelle pour ces deux problèmes consiste à configurer le CPE DSL avec l'utilisation de l'interface de modèle virtuel comme décrit dans la configuration.

Des correctifs pour ces deux problèmes sont prévus pour le logiciel Cisco IOS Version 12.2(4)T. Après cette version, une version mise à jour de ce document est publiée afin d'afficher la configuration de l'interface de numérotation comme une autre option.

Vérification

Cette section fournit les informations que vous pouvez utiliser afin de confirmer que votre configuration fonctionne correctement.

Plusieurs commandes **show** peuvent être utilisées afin de vérifier que la session IPSec est établie entre les homologues. Les commandes ne sont nécessaires que sur les homologues IPSec, dans ce cas les gammes Cisco 2600 et 3600.

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 crypto engine connections active** - Affiche chaque SA de phase 2 créée et la quantité de trafic envoyée.
- **show crypto ipsec sa** - Affiche la SA IPSec construite entre homologues.

Voici un exemple de sortie de commande pour la commande **show crypto engine connections active**.

show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	<none>	<none>	set	HMAC_SHA+DES_56_CB	0	0
200	Virtual-Templat1	10.1.100.101	set	HMAC_SHA	0	4
201	Virtual-Templat1	10.1.100.101	set	HMAC_SHA	4	0

Voici un exemple de sortie de commande pour la commande **show crypto ipsec sa**.

show crypto ipsec sa

```
Interface: Virtual-Templat1
Crypto map tag: vpn, local addr. 10.1.100.101

Local ident (addr/mask/prot/port): (1.1.1.0/255.255.255.0/0/0)
Remote ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)
Current_peer: 10.1.1.5
  PERMIT, flags= {origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr failed: 0, # pkts decompress failed: 0
#send errors 11, #recv errors 0

local crypto endpt: 10.1.100.101, remote crypto endpt.: 10.1.1.5
path mtu 1500, media mtu 1500
current outbound spi: BB3629FB

inbound esp sas:
spi: 0x70C3B00B(1891872779)
  transform: esp-des, esp-md5-hmac
  in use settings ={Tunnel,}
  slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
  sa timing: remaining key lifetime (k/sec): (4607999/3446)
  IV size: 8 bytes
  Replay detection support: Y

Inbound ah sas:

Inbound pcp sas:

Outbound esp sas:
Spi: 0xBB3629FB(3140889083)
  Transform: esp-des, esp-md5-hmac
  In use settings ={Tunnel,}
  Slot:0, conn id: 2001, flow_id: 2, crypto map: vpn
  Sa timing: remaining key lifetime (k/sec): (4607999/3446)
  IV size: 8bytes
  Replay detection support: Y

Outbound ah sas:

Outbound pcp sas:
```

Dépannage

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

Le message « Modem state = 0x8 » qui est signalé par la commande **debug atm events** signifie

généralement que la carte WIC1-ADSL ne peut pas recevoir la détection de porteuse à partir du DSLAM connecté. Dans ce cas, le client doit vérifier que le signal DSL est provisionné sur les deux câbles du milieu par rapport au connecteur RJ11. Certains opérateurs téléphoniques fournissent le signal DSL sur les deux broches extérieures à la place.

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'émettre des commandes **debug**, reportez-vous aux [Informations importantes sur les commandes de débogage](#).

Attention : N'exécutez pas le débogage sur un réseau actif. Le volume d'informations affiché peut surcharger votre routeur au point où aucun flux de données et aucun message CPUHOG ne sont émis.

- **debug crypto ipsec** — Affiche des événements IPsec.
- **debug crypto isakmp**—Affichage de messages d'événements IKE.

Résumé

La mise en oeuvre d'IPSec sur une connexion ADSL fournit une connexion réseau sécurisée et fiable entre les filiales et les sites centraux. L'utilisation de la gamme Cisco 2600/3600 avec les modules ADSL-WIC et de cryptage matériel offre un coût d'acquisition moindre au client, car ADSL et IPSec peuvent désormais être réalisés dans une solution de routeur unique. La configuration et les mises en garde répertoriées dans ce document doivent servir de ligne directrice de base pour configurer ce type de connexion.

Informations connexes

- [Présentation du chiffrement IPSec \(IP Security\)](#)
- [Routeurs de la gamme Cisco 2600](#)
- [Réseaux privés virtuels](#)
- [Support technique DSL et LRE](#)
- [Prise en charge des produits de passerelles universelles](#)
- [Numérotation et accès de l'assistance technique](#)
- [Support technique - Cisco Systems](#)