# ADSL-WIC とハードウェア暗号化モジュールを使用する Cisco 2600/3600 上 で IPSec Over ADSL を設定する方法

## 目次



## 概要

インターネットが拡大するにつれ、ブランチ オフィスでは、信頼性が高く安全な中央サイトへの接続が必要になります。 バーチャル プライベート ネットワーク（VPN）は、インターネット経由で転送される際のリモート オフィスと中央サイト間の情報を保護します。 IP Security（IPSec）を使用して、これらの VPN を通過するデータが確実に暗号化されるようにすることができます。 暗号化はネットワーク セキュリティの別のレイヤを提供します。

この図は典型的な IPSec VPN を示します。 いくつかのリモートアクセスおよびサイト間接続はブランチ オフィスとセントラルサイト間で複雑です。 通常、従来のWAN はフレーム リレーのような、ISDN リンクし、モデムダイヤルアップはサイトの間で提供されます。 これらの接続は高い一度だけプロビジョニング料金および高い月極料金を含むことができます。 また、ISDN およびモデムユーザのため、そこに長い接続時間である場合もあります。

Asymmetric Digital Subscriber Line （ADSL）はこれらの従来のWAN リンクに常時接続を、低価格な代替提供します。 ADSLリンク上の IPSec 暗号化されたデータはセキュアおよび信頼できる接続を提供し、顧客を通貨保存します。 ブランチ オフィスの従来 の ADSL Customer Premises Equipment （CPE） セットアップは IPSecトラフィックを起こし、終えるデバイスに接続する ADSL モデムを必要とします。 この図は典型的な ADSL ネットワークを示します。

Cisco 2600 および 3600 ルータ サポート ADSL WANインターフェイスカード（WIC-1ADSL）。この WIC-1ADSL はブランチ オフィスの必要を満たすように設計されているマルチサービスおよ

びリモートアクセス ソリューションです。 WIC-1ADSL およびハードウェア暗号化モジュールの概要はシングル ルータ ソリューションのブランチ オフィスの IPSec および DSL のためのデマンドを達成します。 WIC-1ADSL は別途の DSL モデムのための必要を省きます。 ハードウェア暗号化モジュールはその暗号化をルータからのプロセス オフロードすると同時にソフトウェアのみの暗号化上のパフォーマンスを 10 倍まで提供します。

これら二つの製品に関する詳細については、Cisco 1700 のための ADSL WAN インターフェイス カードを、2600、Cisco 1700、2600、3600、および 3700 シリーズ用の 3700 シリーズ モジュラ アクセス ルータおよび仮想プライベートネットワークモジュール参照すれば。

# 前提条件

## 要件

このドキュメントに関する固有の要件はありません。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

**Cisco 2600/3600 シリーズ ルータ:**

- Cisco IOS® ソフトウェア リリース 12.1(5)YB Enterprise Plus トリプル DES 機能セット
- のための DRAM 64 MB Cisco 2600 シリーズ、のための DRAM 96 MB Cisco 3600 シリーズ
- のためのフラッシュ 16 MB Cisco 2600 シリーズ、のためのフラッシュ 32 MB Cisco 3600 シリーズ
- WIC-1ADSL
- ハードウェア暗号化モジュールのための AIM-VPN/BP および AIM-VPN/EP Cisco 2600 シリーズCisco 3620/3640 のための NM-VPN/MPCisco 3660 のための AIM-VPN/HP

**Cisco 6400 シリーズ:**

- Cisco IOS ソフトウェア リリース 12.1(5)dc1
- DRAM 64 MB
- フラッシュ 8 MB

**Cisco 6160 シリーズ:**

- Cisco IOS software release 12.1(7)da2
- DRAM 64 MB
- フラッシュ 16 MB

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、コマンドを使用する前にその潜在的な影響について確実に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 設定

このセクションには、このドキュメントで説明している機能を設定する際に利用できる情報が記載されています。

**注:** このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

## ネットワーク図

この資料はこのダイアグラムを示されているネットワーク セットアップを使用します。

このテストは典型的な支店 の 環境で ADSL を使用する IPSec VPN 接続を模倣します。

ADSL-WIC およびハードウェア暗号化モジュールが付いている Cisco 2600/3600 は Cisco 6160 まで digital subscriber line access multiplexer （DSLAM）をトレインします。 Cisco 6400 はその PPP セッションを Cisco 2600 ルータからの開始終了する集約デバイスとして使用されます。 IPSecトンネルは CPE 2600 で起き、セントラル オフィスの Cisco 3600 で、このシナリオの IPSec ヘッドエンド デバイス終わります。 ヘッドエンド デバイスは個々のピアリングの代りにあらゆるクライアントからの接続を許可するために設定されます。 ヘッドエンド デバイスはまた事前共有キーとおよびトリプル DES および Edge Service Processor （ESP）だけ-セキュアハッシュアルゴリズム （SHA） - Hash-Based Message Authentication Code （HMAC）テストされます。

## 設定

このドキュメントでは、次の設定を使用します。

- Cisco 2600 ルータ
- IPSec ヘッドエンド デバイス- Cisco 3600 ルータ
- Cisco 6160 DSLAM
- Cisco 6400 Node Route Processor（NRP; ノード ルート プロセッサ）

コンフィギュレーションについてのこれらのポイントに注意して下さい:

- 事前共有キーは使用されます。 IPSecセッションをマルチプルピアに設定するために、複数のキー定義 ステートメントを定義して下さいダイナミック暗号マップを設定する必要があります。 すべてのセッション 共有が単一 キー、0.0.0.0 のピアアドレスを使用する必要があれば。
- 設定 される トランスフォームは ESP か、Authentication Header （AH）、または二重 認証のためのその両方のために定義することができます。
- 少なくとも 1 つの暗号ポリシー 定義はピアごとに定める必要があります。 クリプト マップは IPSecセッションを作成するのに使用するピアをことにします。 デシジョンはアクセス リストで定義されるアドレス一致に基づいています。 この場合、それは access-list 101 です。
- クリプト マップは物理インターフェイス（インターフェイス ATM 0/0 この場合）およびバーチャル テンプレート両方のために定義する必要があります。
- この資料で表記される設定は DSL接続上の IPSecトンネルだけ論議します。 追加 の セキュリティ 機能はおそらく必要ネットワークが脆弱ではないことを確認するためです。 これらのセキュリティ機能は外部ユニットまたは IOSファイアウォール 機能セットのファイアウォールの追加アクセス コントロール リスト（ACL）、ネットワーク アドレス変換（NAT）およ

び使用を含むことができます。 これらの機能のそれぞれはルータに出入して非 IPSec トラフィックを制限するために使用することができます。

### Cisco 2600 ルータ

```
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
```

### IPSec ヘッドエンド デバイス- Cisco 3600 ルータ

```
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
```

### Cisco 6160 DSLAM

```
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. !
```

## Cisco 6400 NRP

```
!
username cisco password cisco
!
vc-class atm pppoa
 encapsulation aal5mux ppp Virtual-template1
 !
 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-Template1
 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
!
```

## 警告

ADSL 接続はバーチャル テンプレートかダイヤラーインターフェイスで設定することができます。

ダイヤラーインターフェイスはサービスプロバイダーからアドレスを受け取るために DSL CPE を設定するために使用されます ( IP アドレスはネゴシエートされます )。 仮想テンプレートインターフェイスは down-down インターフェイスで、DSL 環境で必要のネゴシエートされたアドレス オプションをサポートしません。 仮想テンプレートインターフェイスは DSL 環境のために最初に実装されました。 現在ダイヤラーインターフェイスは DSL CPE 側の推奨されるコンフィギュレーションです。

2 つの問題は IPSec のダイヤラーインターフェイスの設定の時にあります:

- Cisco バグ ID CSCdu30070 （登録ユーザのみ）—ソフトウェアのみの IPSec over DSL: DSL ダイヤラーインターフェイスのインプットキュー ウェッジ。
- Cisco バグ ID CSCdu30335 （登録ユーザのみ）—ハードウェア ベース IPSec over DSL: ダイヤラーインターフェイスのインプットキュー ウェッジ。

両方の問題のための現在の回避策は設定に記述されているように仮想テンプレートインターフェイスの使用で DSL CPE を設定することです。

両方の問題のための修正は Cisco IOS ソフトウェア リリース 12.2(4)T のために計画されます。別のオプションとしてダイヤラインターフェイスコンフィギュレーションを示すためにこのリリースが、この資料の更新バージョン掲示された後。

## 確認

このセクションは設定はきちんと機能することを確認するために使用できる情報を提供します。

複数の **show コマンドは** IPSecセッションが同位の間で設定されることを確認するために使用することができます。 コマンドは IPSec ピアでだけ必要、この場合 Cisco 2600 および 3600 シリーズです。

特定の **show** コマンドは、Output Interpreter Tool （登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show crypto engine connections active**：確立されたフェーズ 2 の各 SA と送信されたトラフィック量を表示します。
- **show crypto ipsec sa** — 同位の間で構築される IPSec SA 示します。

これは **show crypto engine connections active コマンド**のためのサンプルコマンド出力です。

```
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-Template1 10.1.100.101 set HMAC_SHA 0 4 201
Virtual-Template1 10.1.100.101 set HMAC_SHA 4 0
```

これは **show crypto ipsec sa コマンド**のためのサンプルコマンド出力です。

**show crypto ipsec sa** Interface: Virtual-Template1 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:

# トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

通常 = **debug atm events コマンド**によって報告される 0x8" メッセージ WIC1-ADSL が接続された DSLAM からキャリア検知を受け取ることができないことを意味します。 この場合、DSL 場合が RJ11 コネクタに関連して中間 2 つのネットワークで提供されることを確認する顧客 の ニーズ。 いくつかの Telco は外部 2 ピンの DSL 場合を代りに提供します。

## トラブルシューティングのためのコマンド

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

**注: debug** コマンドを発行する前に、『debug コマンドの重要な情報』を参照してください。

**注意**： 実稼働中 の ネットワークのデバッグを実行しないで下さい。 情報の音量はデータフローおよび CPUHOG メッセージが発行されないポイントに表示する ルータを過剰にすることができます。

- **debug crypto ipsec**：IPSec イベントを表示します。
- **debug crypto isakmp**：IKE イベントに関するメッセージを表示します。

# 要約

ADSL接続上の IPSec の実装はブランチ オフィスとセントラルサイト間のセキュアおよび高信頼性ネットワーク接続を提供します。 ADSL および IPSec として顧客への所有権の ADSL-WIC およびハードウェア暗号化モジュール提供より低い コストの Cisco 2600/3600 シリーズの使用はシングル ルータ ソリューションで今達成することができます。 基本的なガイドラインとしてこの接続の種類を設定するのに動作するこのペーパー必要にリストされている設定および警告。

# 関連情報

- IP セキュリティ（IPSec）暗号化の概要
- Cisco 2600 シリーズ ルータ
- 仮想プライベート ネットワーク（VPN）
- DSL および LRE の技術サポート

- Universal Gateways 製品サポート
- ダイヤルおよびアクセスに関するサポート ページ
- テクニカルサポート - Cisco Systems