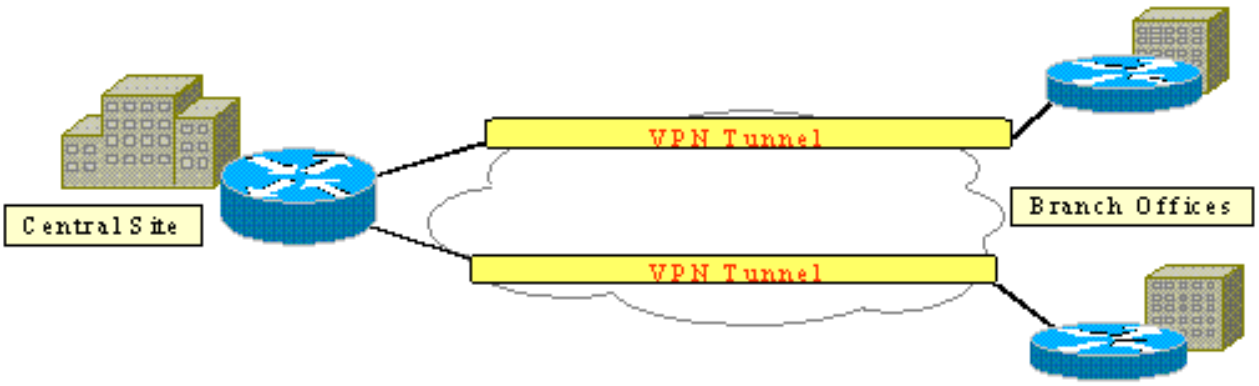
ADSL-WIC とハードウェア暗号化モジュールを使用する Cisco 2600/3600 上 で IPSec Over ADSL を設定する方法

内容

概要
前提条件
要件
使用するコンポーネント
表記法
設定
ネットワーク図
設定
警告
確認
トラブルシュート
トラブルシューティングのためのコマンド
要約
関連情報

概要

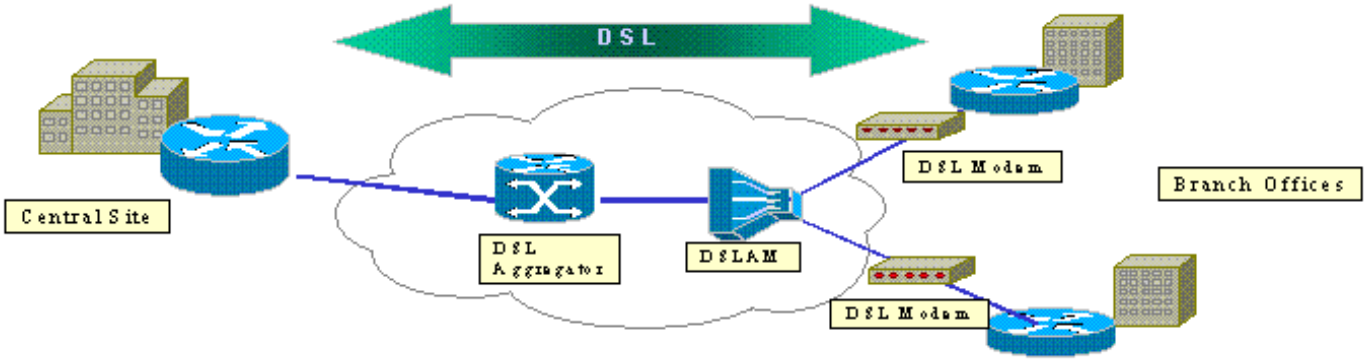
インターネットが拡大するにつれ、ブランチ オフィスでは、信頼性が高く安全な中央サイトへの接続が必要になります。バーチャル プライベート ネットワーク（VPN）は、インターネット経由で転送される際のリモート オフィスと中央サイト間の情報を保護します。IP Security（IPSec）を使用して、これらの VPN を通過するデータが確実に暗号化されるようにすることができます。暗号化はネットワーク セキュリティの別のレイヤを提供します。



次の図に、一般的なIPSec VPNを示します。ブランチオフィスと中央サイトの間には、多数のリ

モートアクセス接続とサイト間接続が含まれています。通常、フレームリレー、ISDN、モデムダイヤルアップなどの従来のWANリンクは、サイト間でプロビジョニングされます。これらの接続には、1回限りのプロビジョニング料金と月額料金が高額になる可能性があります。また、ISDNおよびモデムユーザの場合、接続時間が長くなる可能性があります。

Asymmetric Digital Subscriber Line（ADSL；非対称デジタル加入者線）は、これらの従来のWANリンクに代わる、常にオンで低コストの選択肢を提供します。ADSLリンク上のIPSec暗号化データは、セキュアで信頼性の高い接続を提供し、お客様のコストを削減します。ブランチオフィスに設置された従来のADSL顧客宅内機器(CPE)には、IPSecトラフィックを発信および終端するデバイスに接続するADSLモデムが必要です。次の図は、一般的なADSLネットワークを示しています。



Cisco 2600および3600ルータは、ADSL WANインターフェイスカード(WIC-1ADSL)をサポートします。 このWIC-1ADSLは、ブランチオフィスのニーズを満たすように設計された、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導入により、ブランチオフィスでのIPSecおよびDSLの需要を1つのルータソリューションで達成できます。WIC-1ADSLにより、別のDSLモデムが不要になります。ハードウェア暗号化モジュールは、ルータから処理する暗号化をオフロードするため、ソフトウェアのみの暗号化よりも最大10倍のパフォーマンスを提供します。

これら2つの製品の詳細については、『Cisco 1700、2600、および3700シリーズモジュラアクセスルータ用ADSL WANインターフェイスカード』および『Cisco 1700、2600、360用のバーチャルプライベートネットワークモジュール』を参照してください0および3700シリーズ。

前提条件

要件

このドキュメントに特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いています。

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 3DESフィーチャセット
- Cisco 2600シリーズではDRAM 64 MB、Cisco 3600シリーズではDRAM 96 MB

- Cisco 2600シリーズではフラッシュ16 MB、Cisco 3600シリーズではフラッシュ32 MB
- WIC-1 ADSL
- ハードウェア暗号化モジュールCisco 2600シリーズ用AIM-VPN/BPおよびAIM-VPN/EPCisco 3620/3640用NM-VPN/MPCisco 3660用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ソフトウェアリリース12.1(7)DA2
- DRAM 64 MB
- フラッシュ16 MB

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドでも、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。

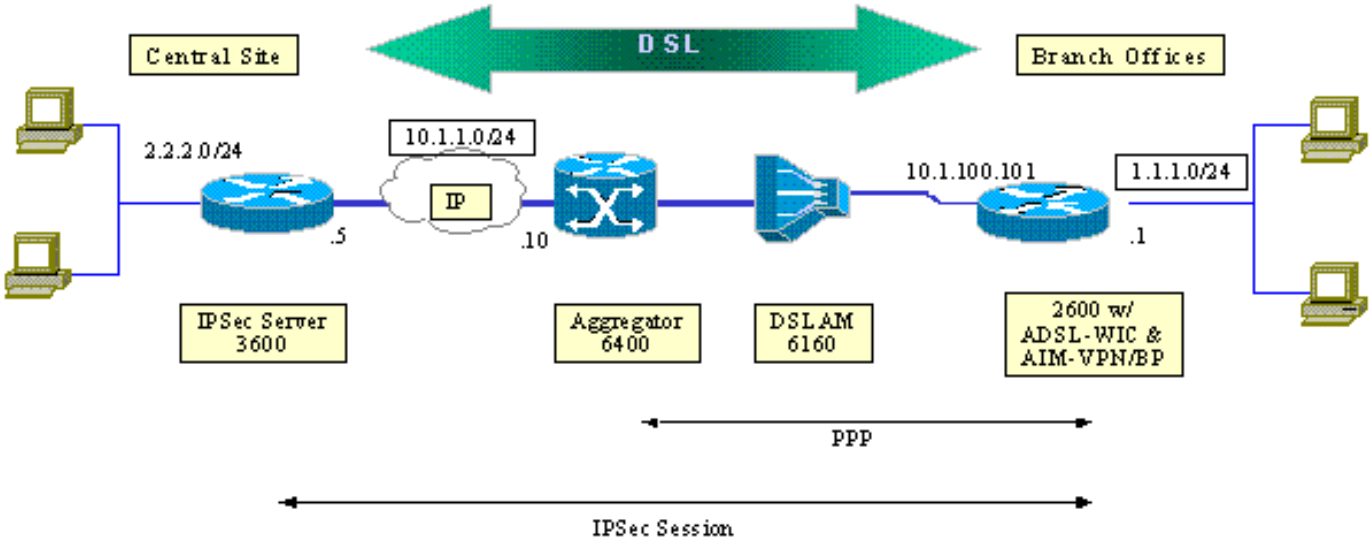
注：このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を使用してください。

ネットワーク図

このドキュメントでは、次の図に示すネットワーク設定を使用します。

このテストでは、一般的なブランチオフィス環境でADSLを使用するIPSec VPN接続をシミュレートします。

ADSL-WICとハードウェア暗号化モジュールを搭載したCisco 2600/3600は、Cisco 6160デジタル加入者線(DSL)アクセスマルチプレクサ(DSLAM)を最大トレインします。 Cisco 6400は、Cisco 2600ルータから開始するPPPセッションを終端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から発信され、セントラルオフィスのCisco 3600（このシナリオではIPSecヘッドエンドデバイス）で終端します。ヘッドエンドデバイスは、個々のピアリングではなく、任意のクライアントからの接続を受け入れるように設定されます。また、ヘッドエンドデバイスは、事前共有キーと3DESおよびEdge Service Processor(ESP)-Secure Hash Algorithm(SHA)-Hash-based Message Authentication Code(HMAC)のみでテストされています。



設定

このドキュメントでは、次の構成を使用します。

- 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)

設定に関しては、次の点に注意してください。

- 事前共有キーが使用されます。複数のピアへのIPSecセッションを設定するには、複数のキー定義ステートメントを定義するか、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が1つのキーを共有する場合は、ピアアドレス0.0.0.0を使用する必要があります。
- トランスフォームセットは、ESP、認証ヘッダー(AH)、またはその両方に対して二重認証を定義できます。
- ピアごとに少なくとも1つの暗号ポリシー定義を定義する必要があります。暗号マップは、IPSecセッションの作成に使用するピアを決定します。この決定は、アクセスリストで定義されたアドレス一致に基づいています。この例では、アクセスリスト101です。
- 暗号マップは、物理インターフェイス (この場合はインターフェイスATM 0/0) と仮想テンプレートの両方に定義する必要があります。
- このドキュメントで説明する設定では、DSL接続上のIPSecトンネルについてのみ説明します。ネットワークに脆弱性が存在しないことを保証するために、追加のセキュリティ機能が必要になる可能性があります。これらのセキュリティ機能には、追加の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)、および外部ユニットまたはIOSファイアウォール機能セットを使用したファイアウォールの使用が含まれます。これらの各機能は、ルータとの間でIPSec以外のトラフィックを制限するために使用できます。

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、仮想テンプレートまたはダイヤラインターフェイスで設定できます。

ダイヤラ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信するようにDSL CPEを設定するために使用されます（IPアドレスが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ダウンインターフェイスであり、DSL環境で必要なネゴシエートされたアドレスオプションはサポートしません。仮想テンプレートインターフェイスは、当初DSL環境に実装されました。現在、ダイヤラインターフェイスはDSL CPE側の推奨設定です。

IPSecを使用したダイヤラインターフェイスの設定時に、次の2つの問題が見つかりました。

- Cisco Bug ID CSCdu30070(登録ユーザ専用):Software-only IPSec over DSL:DSLダイヤラインターフェイスの入力キューウェッジ。
- Cisco Bug ID CSCdu30335(登録ユーザ専用)：ハードウェアベースのIPSec over DSL:ダイヤラインターフェイスの入力キューウェッジ

両方の問題の現在の回避策は、設定で説明されているように、仮想テンプレートインターフェイスを使用してDSL CPEを設定することです。

両方の問題に対する修正は、Cisco IOSソフトウェアリリース12.2(4)Tで予定されています。このリリース以降、ダイヤラインターフェイスの設定を別のオプションとして表示するために、このドキュメントの更新バージョンが公開されています。

確認

このセクションでは、設定が正しく動作していることを確認するために使用できる情報を提供します。

ピア間でIPSecセッションが確立されていることを確認するために、いくつかのshowコマンドを使用できます。これらのコマンドは、IPSecピア（この場合はCisco 2600および3600シリーズ）でのみ必要です。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- **show crypto engine connections active**：構築された各フェーズ2 SAと送信されたトラフィックの量を表示します。
- **show crypto ipsec sa**：ピア間で構築されたIPSec SAを表示します。

次に、**show crypto engine connections active**コマンドの**コマンド出力例を示**します。

```
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
```

次に、**show crypto ipsec saコマンドのコマンド出力例を示**します。

```
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:
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

「`Modem state = 0x8`**debug atm eventsコマンドで報告さ**れるのは、通常、WIC1-ADSLが接続されたDSLAMからキャリア検出(CD)を受信できないという意味です。この状況では、DSL信号がRJ11コネクタに関連して中央の2本のワイヤにプロビジョニングされていることを確認する必要があります。一部の電話会社は、外部の2つのピンにDSL信号をプロビジョニングします。

トラブルシューティングのためのコマンド

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

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：ライブネットワークではデバッグを実行しないでください。表示される情報の量は、データフローやCPUHOGメッセージが発行されない状態までルータを過負荷にする可能性があります。

- **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接続を介したIPSecの実装は、ブランチオフィスと中央サイト間のセキュアで信頼性の高いネットワーク接続を提供します。ADSL-WICおよびハードウェア暗号化モジュールとともにCisco 2600/3600シリーズを使用すると、ADSLおよびIPSecを1つのルータソリューションで実現できるため、お客様の所有コストが低くなります。この文書に記載されている設定と警告は、このタイプの接続を設定するための基本的なガイドラインとして役立つ必要があります。

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
- バーチャルプライベートネットワーク
- DSL および LRE の技術サポート
- ユニバーサルゲートウェイ製品のサポート
- 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