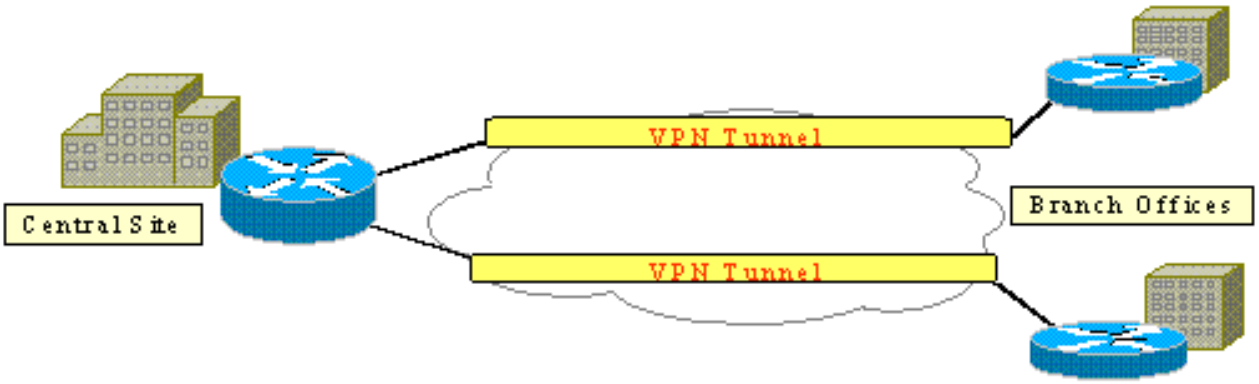
在具有ADSL-WIC和硬體加密模組的Cisco 2600/3600上配置IPSec Over ADSL

目錄

簡介

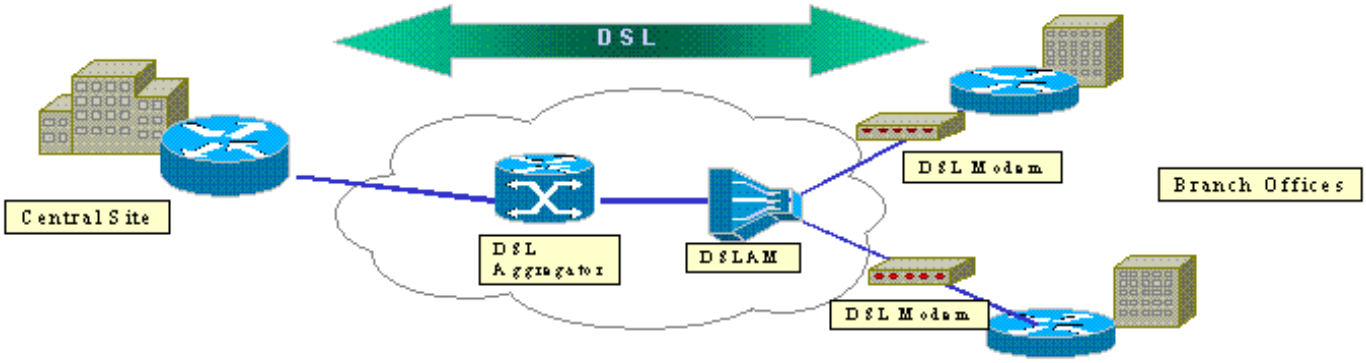
隨著Internet的擴展，分支機構要求其到中心站點的連線既可靠又安全。虛擬專用網路(VPN)可在資訊通過Internet傳輸時，保護遠端辦公室和中心站點之間的資訊。IP安全(IPSec)可用於保證通過這些VPN的資料得到加密。加密提供了另一層網路安全。



下圖顯示了典型的IPSec VPN。分支機構和中心站點之間涉及許多遠端訪問和站點到站點連線。通常，傳統的WAN鏈路（如幀中繼、ISDN和數據機撥號）會在站點之間調配。這些連線可能需要支付昂貴的一次性調配費用和昂貴的月費。此外，對於ISDN和資料機使用者，連線時間可能會很長。

非對稱式數位使用者線路(ADSL)為這些傳統WAN鏈路提供永遠線上、低成本的替代方案。通過

ADSL鏈路的IPSec加密資料可提供安全可靠的連線，並為客戶節省資金。在分支機構中設定的傳統ADSL客戶端裝置(CPE)需要一個ADSL數據機，該數據機連線到發起和終止IPSec流量的裝置。下圖顯示了典型的ADSL網路。



Cisco 2600和3600路由器支援ADSL WAN介面卡(WIC-1ADSL)。 此WIC-1ADSL是一種多服務和遠端訪問解決方案，旨在滿足分支機構的需求。WIC-1ADSL和硬體加密模組的引入滿足了分支機構對單一路由器解決方案中IPSec和DSL的需求。WIC-1ADSL無需使用單獨的DSL數據機。當硬體加密模組從路由器解除安裝處理加密時，與純軟體加密相比，該模組可提供高達10倍的效能。

有關這兩個產品的詳細資訊，請參閱適用於Cisco 1700、2600和3700系列模組化接入路由器的ADSL WAN介面卡和適用於Cisco 1700、2600、3600和3700系列的虛擬專用網路模組。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

Cisco 2600/3600系列路由器：

- Cisco IOS®軟體版本12.1(5)YB Enterprise PLUS 3DES功能集
- DRAM 64 MB（Cisco 2600系列）、DRAM 96 MB（Cisco 3600系列）
- Cisco 2600系列的快閃記憶體16 MB，Cisco 3600系列的快閃記憶體32 MB
- WIC-1 ADSL
- 硬體加密模組適用於思科2600系列的AIM-VPN/BP和AIM-VPN/EP適用於Cisco 3620/3640的NM-VPN/MP適用於Cisco 3660的AIM-VPN/HP

思科6400系列：

- Cisco IOS軟體版本12.1(5)DC1
- DRAM 64 MB
- 快閃記憶體8 MB

思科6160系列：

- Cisco IOS軟體版本12.1(7)DA2
- DRAM 64 MB
- 快閃記憶體16 MB

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果在實際網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

本節提供可用於設定本檔案中所述功能的資訊。

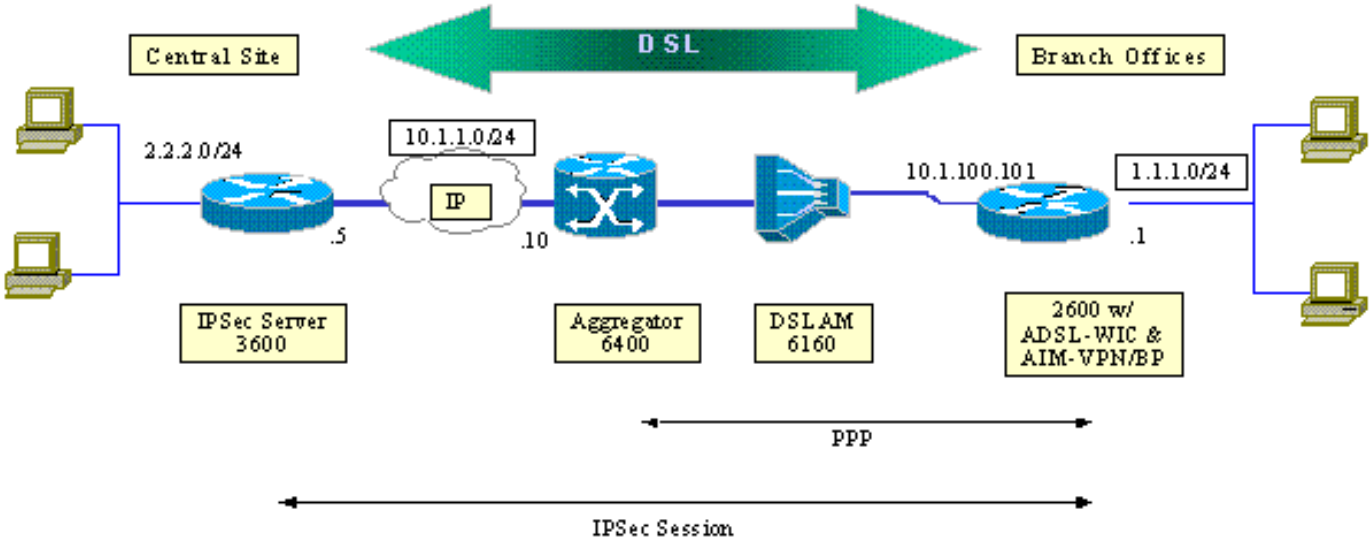
注意：若要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本文檔使用如圖所示的網路設定。

此測試模擬在典型分支機構環境中使用ADSL的IPSec VPN連線。

具備ADSL-WIC和硬體加密模組的Cisco 2600/3600可培訓多達Cisco 6160數字使用者線接入複用器(DSLAM)。 Cisco 6400用作終止從Cisco 2600路由器發起的PPP會話的聚合裝置。IPSec隧道源自CPE 2600，終止於中心辦公室的Cisco 3600，在此場景中為IPSec前端裝置。頭端裝置設定為接受來自任何使用者端的連線，而不是單獨的對等。頭端裝置也僅使用預共用金鑰和3DES及邊緣服務處理器(ESP) — 安全雜湊演演算法(SHA) — 雜湊型訊息驗證碼(HMAC)進行測試。



組態

本檔案會使用以下設定：

- 思科2600路由器
- IPSec頭端裝置 — Cisco 3600路由器
- Cisco 6160 DSLAM
- 思科6400節點路由處理器(NRP)

請注意有關配置的以下幾點：

- 使用預共用金鑰。為了設定到多個對等體的IPSec會話，必須定義多個金鑰定義語句，或者需要配置動態加密對映。如果所有會話共用一個金鑰，則必須使用0.0.0.0的對等地址。
- 轉換集可以為ESP、身份驗證報頭(AH)定義，也可以為雙重身份驗證定義。
- 每個對等體必須至少定義一個加密策略定義。加密對映決定用於建立IPSec會話的對等裝置。決定取決於訪問清單中定義的地址匹配。在本例中，它是access-list 101。
- 必須為物理介面（本例中為ATM 0/0介面）和虛擬模板定義加密對映。
- 本文檔中顯示的配置僅討論通過DSL連線的IPSec隧道。為了確保您的網路不易受攻擊，可能需要額外的安全功能。這些安全功能可能包括額外的存取控制清單(ACL)、網路位址轉譯(NAT)，以及將防火牆與外部裝置或IOS防火牆功能集一起使用。可以使用其中每個功能來限制進出路由器的非IPSec流量。

思科2600路由器

```
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頭端裝置 — Cisco 3600路由器

```
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
!
```

注意事項

可以使用虛擬模板或撥號器介面配置ADSL連線。

撥號器介面用於配置DSL CPE以從服務提供商接收地址（IP地址是協商的）。虛擬模板介面是下行介面，不支援在DSL環境中必需的協商地址選項。虛擬模板介面最初是針對DSL環境實施的。目前撥號器介面是DSL CPE端上的建議組態。

在使用IPSec配置撥號器介面時發現兩個問題：

- Cisco錯誤ID CSCdu30070(僅限註冊客戶) — 僅軟體的IPSec over DSL:dsl撥號器介面上的輸入隊列楔形。
- Cisco錯誤ID CSCdu30335(僅限註冊客戶) — 使用DSL的基於硬體的IPSec:撥號器介面上的輸入隊列楔形。

這兩個問題的當前解決方法是使用配置中所述的虛擬模板介面配置DSL CPE。

計畫在Cisco IOS軟體版本12.2(4)T中修復這兩個問題。在此版本發佈後，將發佈此文檔的更新版本，以便將撥號器介面配置顯示為另一個選項。

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

可使用幾個**show**命令來驗證對等體之間是否建立了IPSec會話。只有在IPSec對等體（本例中為Cisco 2600和3600系列）上才需要這些命令。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

- **show crypto engine connections active** — 顯示已建立的每個階段2 SA和已傳送的流量量。
- **show crypto ipsec sa** — 顯示對等體之間構建的IPSec SA。

以下是**show crypto engine connections active**命令的命令輸出示例。

```
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
```

以下是**show crypto ipsec sa**命令的輸出示例。

```
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:
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

debug atm events命令報告的`= 0x8`消息通常表示WIC1-ADSL無法從連線的DSLAM接收載波檢測。在這種情況下，客戶需要檢查DSL訊號是否設定在相對於RJ11聯結器的中間兩根電線上。某些Telcos在外部兩個引腳上提供DSL訊號。

指令疑難排解

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：發出debug命令之前，請參閱有關Debug命令的重要資訊**。**

注意：請勿在即時網路上運行調試。顯示的資訊量可能使路由器過載，以至於無法傳送資料流和CPUHOG消息。

- **debug crypto IPSec** — 顯示IPSec事件。
- **debug crypto Isakmp** — 顯示有關IKE事件的消息。

摘要

通過ADSL連線實施IPSec可在分支機構和中心站點之間提供安全可靠的網路連線。將Cisco 2600/3600系列與ADSL-WIC和硬體加密模組配合使用，為客戶降低了擁有成本，因為ADSL和IPSec現在可以在單個路由器解決方案中實現。本文列出的配置和注意事項可作為建立此類連線的基本指南。

相關資訊

- IP安全(IPSec)加密簡介
- Cisco 2600系列路由器
- 虛擬私人網路
- DSL和LRE技術支援
- 通用閘道產品支援
- 撥號和存取技術支援
- 技術支援 - Cisco Systems