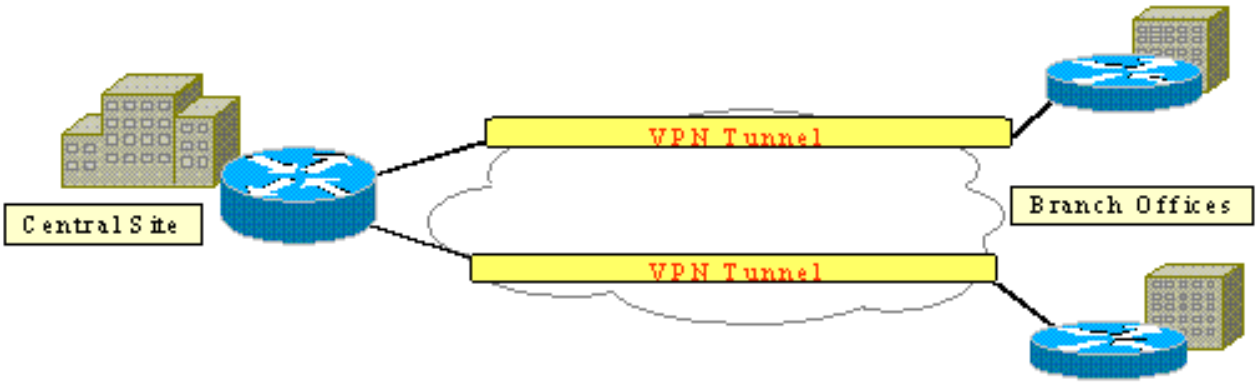
在配有 ADSL-WIC 与硬件加密模块的 Cisco 2600/3600 上配置 ADSL 上的 IPSec

目录

简介

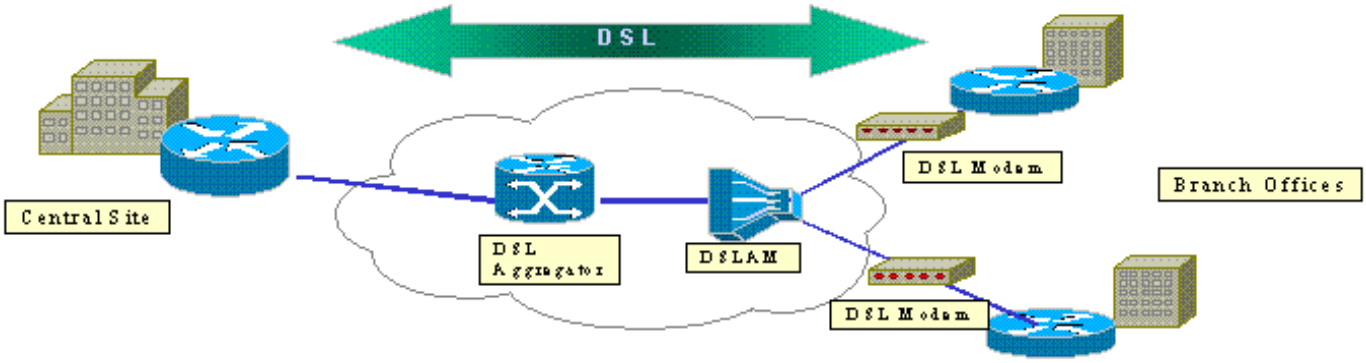
随着Internet的扩展，分支机构要求其与中心站点的连接既可靠又安全。虚拟专用网络(VPN)可在远程办公室和中心站点之间通过互联网传输时保护信息。IP安全(IPSec)可用于保证通过这些VPN的数据被加密。加密提供了另一层网络安全。



此图显示了典型的IPSec VPN。分支机构和中心站点之间涉及许多远程访问和站点到站点连接。通常，传统WAN链路（如帧中继、ISDN和调制解调器拨号）在站点之间调配。这些连接可能需要支付昂贵的一次性调配费用和昂贵的月费。此外，对于ISDN和调制解调器用户，连接时间可能很长。

非对称数字用户线路(ADSL)提供了这些传统WAN链路的无间断、低成本的替代方案。IPSec加密数

据通过ADSL链路提供安全可靠的连接，为客户节省资金。在分支机构中设置的传统ADSL用户驻地设备(CPE)需要ADSL调制解调器，该调制解调器连接到发起和终止IPSec流量的设备。此图显示了典型的ADSL网络。



Cisco 2600和3600路由器支持ADSL广域网接口卡(WIC-1ADSL)。 此WIC-1ADSL是多服务和远程访问解决方案，旨在满足分支机构的需求。WIC-1ADSL和硬件加密模块的引入在单个路由器解决方案中满足了分支机构对IPSec和DSL的需求。WIC-1ADSL无需单独的DSL调制解调器。硬件加密模块在卸载路由器处理的加密时，其性能是纯软件加密的十倍。

有关这两种产品的详细信息，请参阅适用于Cisco 1700、2600和3700系列模块化接入路由器的ADSL广域网接口卡和适用于Cisco 1700、2600和360的虚拟专用网络模块0和3700系列。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

Cisco 2600/3600 系列路由器:

- 思科IOS®软件版本12.1(5)YB Enterprise PLUS 3DES功能集
- Cisco 2600系列的DRAM 64 MB，Cisco 3600系列的DRAM 96 MB
- Cisco 2600系列闪存16 MB，Cisco 3600系列闪存32 MB
- WIC-1 ADSL
- 硬件加密模块AIM-VPN/BP和AIM-VPN/EP，适用于Cisco 2600系列NM-VPN/MP，用于思科3620/3640适用于Cisco 3660的AIM-VPN/HP

Cisco 6400 系列：

- 思科IOS软件版本12.1(5)DC1
- DRAM 64 MB
- 闪存 8 MB

Cisco 6160 系列：

- 思科IOS软件版本12.1(7)DA2
- DRAM 64 MB
- 闪存 16 MB

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

配置

在此部分，您可以看到本文所描述功能的配置信息。

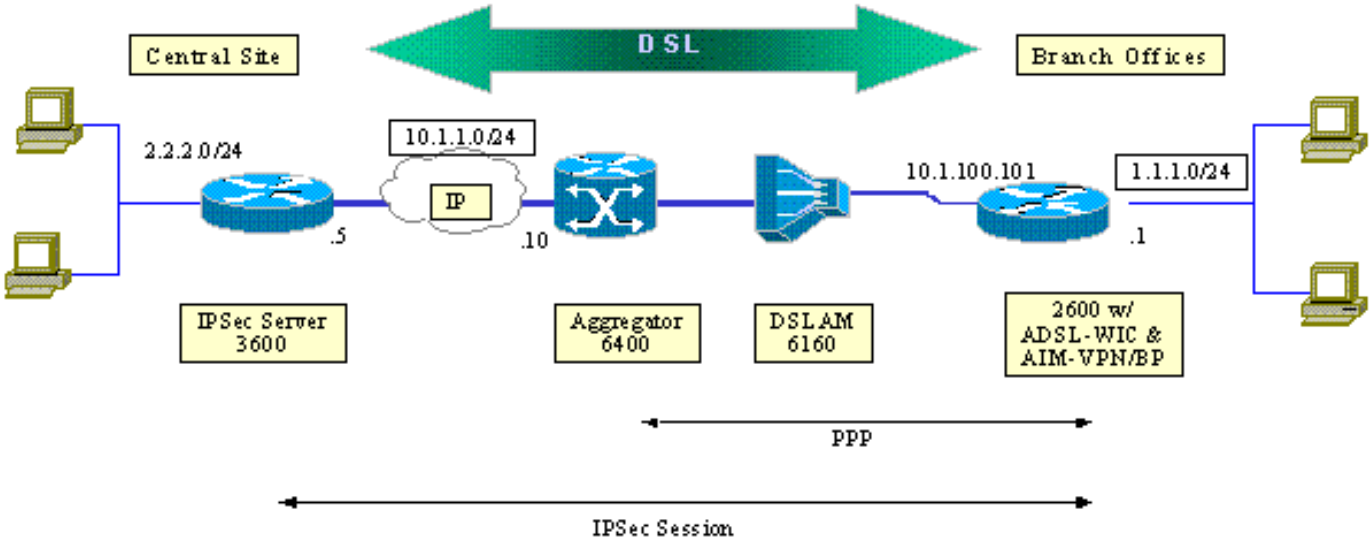
注意：要查找有关本文档中使用的命令的其他信息，请使用命令查找工具(仅注册客户)。

网络图

本文档使用下图所示的网络设置。

本测试模拟在典型分支机构环境中使用ADSL的IPSec VPN连接。

Cisco 2600/3600配备ADSL-WIC和硬件加密模块，可培训至Cisco 6160数字用户线路接入复用器(DSLAM)。 Cisco 6400用作汇聚设备，用于终止从Cisco 2600路由器启动的PPP会话。IPSec隧道始于CPE 2600，终止于中心局（本场景中的IPSec头端设备）的Cisco 3600。头端设备配置为接受来自任何客户端的连接，而不是单个对等。头端设备也仅使用预共享密钥和3DES和边缘服务处理器(ESP) — 安全散列算法(SHA) — 基于散列的消息验证代码(HMAC)进行测试。



配置

本文档使用以下配置：

- Cisco 2600 路由器
- IPSec头端设备 — Cisco 3600路由器
- 思科6160 DSLAM
- 思科6400节点路由处理器(NRP)

请注意以下有关配置的要点：

- 使用预共享密钥。要设置到多个对等体的IPSec会话，必须定义多个密钥定义语句，或者需要配置动态加密映射。如果所有会话共享一个密钥，则必须使用对等地址0.0.0.0。
- 转换集可以为ESP、身份验证报头(AH)或两者定义，以进行双重身份验证。
- 每个对等体必须至少定义一个加密策略定义。加密映射决定了用于创建IPSec会话的对等体。该决定基于访问列表中定义的地址匹配。在本例中，它是access-list 101。
- 必须为物理接口（本例中为接口ATM 0/0）和虚拟模板定义加密映射。
- 本文档中介绍的配置仅讨论通过DSL连接的IPSec隧道。可能需要其他安全功能来确保您的网络不易受攻击。这些安全功能可包括其他访问控制列表(ACL)、网络地址转换(NAT)，以及将防火墙与外部设备或IOS防火墙功能集配合使用。可以使用这些功能中的每一项来限制进出路由器的非IPSec流量。

Cisco 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头端设备 — 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
```

思科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
!
```

注意事项

ADSL连接可以配置虚拟模板或拨号器接口。

拨号器接口用于配置DSL CPE以从服务提供商接收地址（IP地址协商）。虚拟模板接口是关闭接口，不支持协商地址选项，这在DSL环境中是必需的。虚拟模板接口最初是为DSL环境实施的。目前，DSL CPE端建议配置拨号器接口。

在配置带IPSec的拨号器接口时发现两个问题：

- Cisco Bug ID CSCdu30070(仅注册客户) — 仅软件IPSec over DSL:DSL拨号器接口上的输入队列楔。
- Cisco Bug ID CSCdu30335(仅注册客户) — 基于硬件的IPSec over DSL:拨号器接口上的输入队列楔。

当前解决这两个问题的方法是使用虚拟模板接口配置DSL CPE，如配置中所述。

针对这两个问题的修复计划用于Cisco IOS软件版本12.2(4)T。此版本发布后，将发布本文档的更新版本，以将拨号器接口配置显示为另一个选项。

验证

本部分提供可用于确认配置是否正常工作的信息。

可以使用**show**命令来验证对等体之间是否已建立IPSec会话。这些命令仅在IPSec对等体（本例中为Cisco 2600和3600系列）上是必需的。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

- **show crypto engine connections active** — 显示每个第2阶段SA构建和发送的流量。
- **show crypto ipsec sa** — 显示对等体之间构建的IPSec SA。

以下是show crypto engine connections active命令**的命令输出**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**命令输出**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:
```

故障排除

本节提供可用于排除配置故障的信息。

debug atm events命"= 0x8"WIC1-ADSLDSLAM在这种情况下，客户需要检查DSL信号是否配置在与RJ11连接器相对的中间两根电线上。有些Telcos将DSL信号调配到外部两个引脚。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

注：在发出debug命**令**之前，请参阅有关debug命令的重要信息。

注意：请勿在实时网络上运行调试。显示的信息量会使路由器过载到没有数据流和CPUHOG消息的点。

- **debug crypto ipsec — 显示 IPSec 事件。**
- **debug crypto isakmp — 显示关于 IKE 事件的消息。**

摘要

通过ADSL连接实施IPSec，可在分支机构和中心站点之间提供安全可靠的网络连接。Cisco 2600/3600系列与ADSL-WIC和硬件加密模块配合使用，为客户提供更低的拥有成本，因为ADSL和IPSec现在可以在单个路由器解决方案中完成。本白皮书中列出的配置和注意事项需要作为建立此类连接的基本指南。

相关信息

- **IP 安全 (IPsec) 加密简介**
- **思科 2600 系列路由器**
- **虚拟专用网络**
- **DSL 和 LRE 技术支持**
- **通用网关产品支持**
- **拨号和接入技术支持**
- **技术支持 - Cisco Systems**