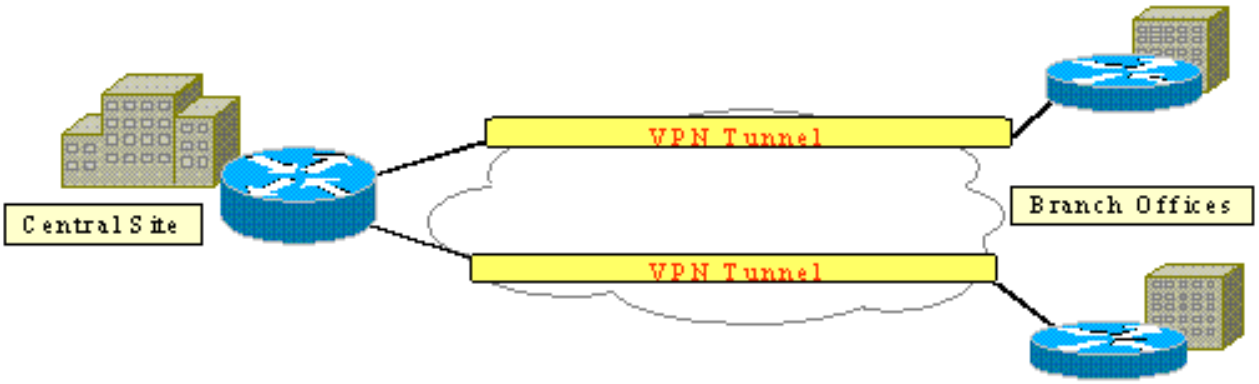
在配有 ADSL-WIC 与硬件加密模块的 Cisco 2600/3600 上配置 ADSL 上的 IPSec

目录

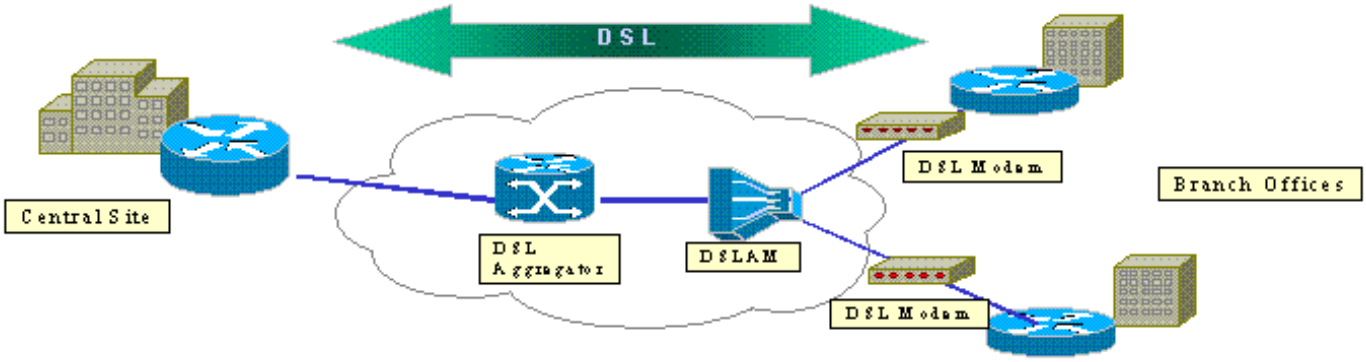
简介

当互联网展开，分支机构需求他们的对中心站点的连接可靠和安全。当在互联网间，移动虚拟专用网络保护在远程办公室和中心站点之间的信息。IP安全能使用保证在这些VPN间通过的数据加密。加密提供网络安全另一块层。



此图显示典型的IPSec VPN。一定数量的远程访问和站点到站点连接是包含的在分支机构和中心站点之间。通常，传统广域网连接例如帧中继， ISDN，并且调制解调器拨号设置在站点之间。这些连接能介入昂贵一次性供应成本和昂贵月费。并且，为ISDN和调制解调器用户，可以有长连接时间。

非对称数字用户线(ADSL)提供不间断工作的，低成本的替代方案对这些传统广域网链路。在ADSL链路的IPSec已加密数据提供安全和可靠的连接并且存客户金钱。一个传统ADSL客户端前置设备(CPE)设置在分支机构要求连接到设备产生并且终止IPSec数据流的ADSL调制解调器。此图显示典型ADSL网络。



Cisco 2600及3600路由器支持ADSL WAN接口卡(WIC-1ADSL)。此WIC-1ADSL是设计的多业务和远程访问解决方案适应分支机构的需要。WIC-1ADSL和硬件加密模块的介绍在单个路由器解决方案的一个分支机构完成对IPSec和DSL的需求。WIC-1ADSL排除需要对于一个分开的DSL调制解调器。硬件加密模块提供十倍在仅软件加密的性能，当卸载从路由器处理的加密。

关于这两产品的更多信息，参考Cisco 1700的ADSL广域网接口卡， 2600和3700系列模块化访问路由器和虚拟专用网络模块Cisco 1700， 2600， 3600和3700系列的。

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：

- Cisco IOS软件版本12.1(5)YB Enterprise Plus 3DES特性组
- Cisco 2600系列的DRAM 64 MB， Cisco 3600系列的DRAM 96 MB
- Cisco 2600系列，闪存32 MB的闪存16 MB Cisco 3600系列的
- WIC-1ADSL
- 硬件加密模块AIM-VPN/BP和AIM-VPN/EP Cisco 2600系列的思科的3620/3640 NM-VPN/MPCisco 3660的AIM-VPN/HP

Cisco 6400系列：

- Cisco IOS软件版本12.1(5)dc1
- DRAM 64 MB
- 闪存8 MB

Cisco 6160系列：

- Cisco 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

有关文档规则的详细信息，请参阅 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。

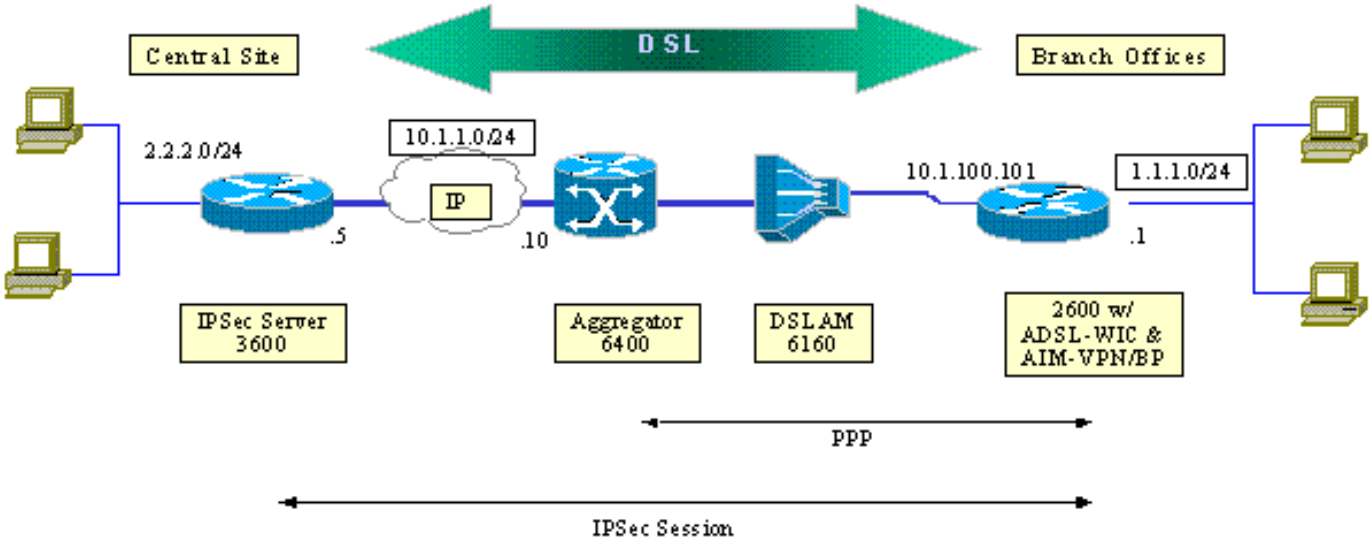
注意： 要查找有关本文档中所使用的命令的详细信息，请使用命令查找工具（仅限注册用户）。

网络图

本文使用显示的网络设置此图表。

此测验模拟在一个典型的分支机构环境使用ADSL的IPSec VPN连接。

Cisco2600/3600用ADSL-WIC和硬件加密模块培训至Cisco 6160数字用户线路访问多路复用器。Cisco 6400使用作为终止PPP会话从Cisco 2600路由器启动的聚合设备。IPSec隧道产生在CPE 2600并且终止在Cisco3600在中心局，在此方案的IPSec头和尾设备。数据转发设备配置接受从所有客户端的连接而不是单个同位体。数据转发设备用预先共享密钥也测试和仅3DES和Edge Service Processor (ESP) -安全哈希算法(SHA) -基于HASH算法的消息认证代码(HMAC)。



配置

本文档使用以下配置：

- Cisco 2600 路由器
- IPSec头和尾设备- Cisco 3600路由器
- Cisco 6160 DSLAM
- Cisco 6400节点路由处理器(NRP)

注意关于配置的这些点：

- 使用预先共享密钥。为了设置IPSec会话对多个对等项，您必须定义多个关键定义语句或您需要配置动态加密映射。如果所有会话共享单个密钥，您必须使用0.0.0.0对等地址。
- 转换集可以为ESP，认证报头(AH)或者两个定义双重身份验证的。
- 至少必须每对等体定义一个加密政策定义。加密映射决定对等体使用创建IPSec会话。决策根据在访问列表定义的地址匹配。在这种情况下，它是access-list 101。
- 必须为物理接口(接口ATM0/0在这种情况下)和虚拟模板定义加密映射。
- 在本文提交的配置讨论在DSL连接的仅一个IPSec隧道。附加安全性功能很可能是需要的为了保证您的网络不易受攻击。这些安全功能能包括另外的访问控制列表(ACL)、网络地址转换(NAT)和使用防火墙与一个外部单元或IOS防火墙特性组。这些功能中的每一个可以用于为了到/从路由器限制IPSec信息数据流。

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头和尾设备- 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
```

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连接可以配置与虚拟模板或拨号接口。

拨号接口用于为了配置DSL CPE收到从服务提供商的一个地址(IP地址协商)。虚拟模板接口是关闭接口，并且不支持协商得到的地址选项，是必要的在DSL环境。虚拟模板接口为DSL环境最初实现。目前拨号接口是在DSL CPE侧的推荐的配置。

两个问题在拨号接口的配置时与IPSec的被找到：

- Cisco Bug ID CSCdu30070 (仅限注册用户) —仅软件IPSec over DSL ：在DSL拨号接口的Input queue楔子。
- Cisco Bug ID CSCdu30335 (仅限注册用户) —基于硬件的IPSec over DSL ：在拨号接口的Input queue楔子。

这两个问题的当前应急方案是配置与使用的DSL CPE虚拟模板接口正如配置所描述。

这两个问题的修正对Cisco IOS软件版本12.2(4)T计划。在此版本，本文一个更新版本被张贴为了显示拨号接口配置作为另一个选项后。

验证

此部分提供您能使用为了确认的信息您的配置适当地工作。

数**显示**命令可以使用为了验证IPSec会话建立在对等体之间。命令是仅必要的在IPSec对等体，在这种情况下Cisco 2600和3600系列。

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** - 显示已建立的每个阶段 2 SA 和已发送的流量。
- **show crypto ipsec sa** —显示SA IPSec被构件在对等体之间。

这是**show crypto engine connections active命令的**示例命令输出。

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

这是**show crypto ipsec sa命令的**示例命令输出。

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

此部分提供您能使用为了排除故障您的配置的信息。

"=由**debug atm events命令**报告的0x8"消息通常意味着WIC1-ADSL无法接收从已连接DSLAM的载波检测。在这种情况下，用户需求检查DSL信号在中间两根金属丝设置相对RJ11连接器。一些Telco设置在外部两管脚的DSL信号。

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。

注意： 在发出 **debug** 命令之前，请参阅有关 debug 命令的重要信息。

警告： 请勿运行在真实网络的调试。显示的音量信息能超载您的路由器到数据流和CPUHOG消息没有发出的点。

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

摘要

IPSec的实施在ADSL连接的提供分支机构和中心站点之间的一个安全和可靠的网络连接。当ADSL和IPSec在单个路由器解决方案，可能当前完成使用Cisco 2600/3600系列用ADSL-WIC和硬件加密模块提供更低成本所有权给客户。在此纸需要和警告列出的配置担当一个基本指南设置此种连接。

相关信息

- IP 安全 (IPsec) 加密简介

- Cisco 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