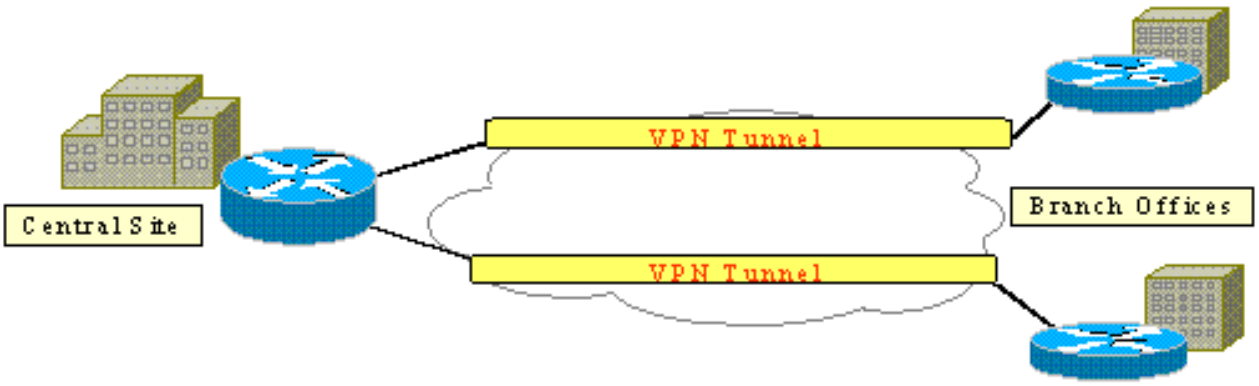
Configuración de IPSec sobre ADSL en un Cisco 2600/3600 con módulos de encripción del hardware y ADSL-WIC.

Contenido

Introducción

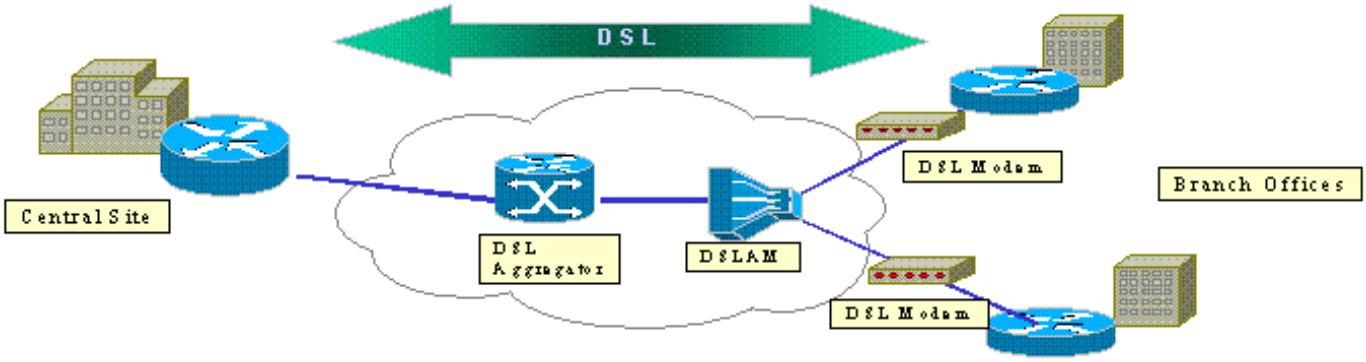
A medida que crece Internet, las sucursales exigen que sus conexiones con los sitios centrales sean confiables y seguras. Las Redes Privadas Virtuales (VPN) protegen la información entre las oficinas remotas y los sitios centrales mientras viaja a través de Internet. IP Security (IPSec) se puede utilizar para garantizar que los datos que pasan a través de estas VPN están cifrados. El cifrado provee otra capa de seguridad de la red.



Esta figura muestra una VPN IPSec típica. Hay varias conexiones de acceso remoto y de sitio a

sitio entre sucursales y sitios centrales. Por lo general, los links WAN tradicionales como Frame Relay, ISDN y marcado de módem se aprovisionan entre los sitios. Estas conexiones pueden implicar una costosa cuota de aprovisionamiento única y costosos cargos mensuales. Además, para los usuarios de ISDN y módem, puede haber tiempos de conexión largos.

La línea de suscriptor digital asimétrico (ADSL) ofrece una alternativa siempre activa y de bajo coste a estos enlaces WAN tradicionales. Los datos cifrados IPSec a través de un enlace ADSL ofrecen una conexión segura y fiable y ahorran dinero a los clientes. Un equipo tradicional de las instalaciones del cliente ADSL (CPE) configurado en una sucursal requiere un módem ADSL que se conecte a un dispositivo que origine y termine el tráfico IPSec. Esta figura muestra una red ADSL típica.



Los routers Cisco 2600 y 3600 admiten la tarjeta de interfaz WAN ADSL (WIC-1ADSL). WIC-1ADSL es una solución de acceso remoto y multiservicio diseñada para satisfacer las necesidades de una sucursal. La introducción de WIC-1ADSL y los módulos de cifrado de hardware satisfacen la demanda de IPSec y DSL en una sucursal en una única solución de router. WIC-1ADSL elimina la necesidad de un módem DSL independiente. El módulo de encripción de hardware proporciona hasta diez veces el rendimiento sobre el encripción sólo de software a medida que descarga el encripción que procesa desde el router.

Para obtener más información sobre estos dos productos, refiérase a Tarjetas de Interfaz WAN ADSL para los Cisco 1700, 2600 y 3700 Series Modular Access Routers y Módulos de Red Privada Virtual para Cisco 1700, 2600, 3600 y 37000 .

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Cisco 2600/3600 Series Routers:

- Conjunto de funciones 12.1(5)YB Enterprise PLUS 3DES del software Cisco IOS®

- DRAM de 64 MB para la serie Cisco 2600, DRAM de 96 MB para la serie Cisco 3600
- Flash de 16 MB para la serie Cisco 2600, Flash de 32 MB para la serie Cisco 3600
- WIC-1 ADSL
- Módulos de cifrado de hardwareAIM-VPN/BP y AIM-VPN/EP para la serie Cisco 2600NM-VPN/MP para el Cisco 3620/3640AIM-VPN/HP para el Cisco 3660

Cisco serie 6400

- Versión 12.1(5)DC1 del software del IOS de Cisco
- DRAM 64 MB
- Flash 8 MB

Cisco serie 6160

- Versión 12.1(7)DA2 del software del IOS de Cisco
- DRAM 64 MB
- Flash 16 MB

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configurar

En esta sección, se le presenta la información que puede utilizar para configurar las funciones descritas en este documento.

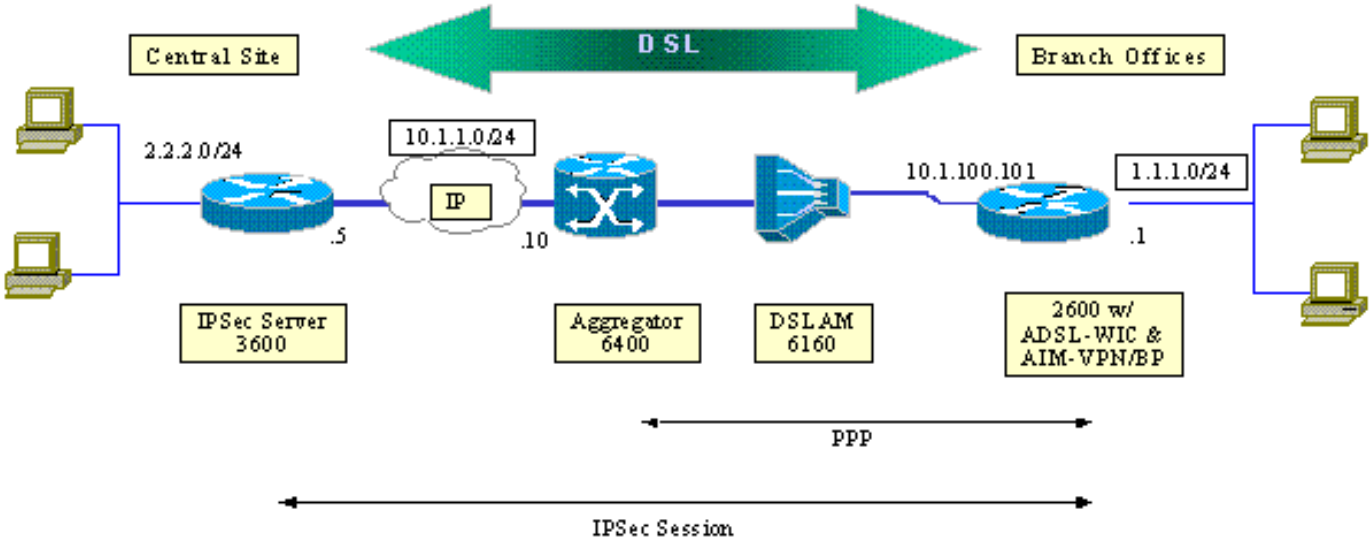
Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la Command Lookup Tool (sólo clientes registrados) .

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en este diagrama.

Esta prueba simula una conexión VPN IPSec que utiliza ADSL en un entorno de sucursal típico.

El Cisco 2600/3600 con ADSL-WIC y el módulo de cifrado de hardware capacita hasta un multiplexor de acceso de línea de suscriptor digital (DSLAM) Cisco 6160. El Cisco 6400 se utiliza como dispositivo de agregación que finaliza una sesión PPP que se inicia desde el router Cisco 2600. El túnel IPSec se origina en el CPE 2600 y termina en el Cisco 3600 en la oficina central, el dispositivo de cabecera IPSec en este escenario. El dispositivo de cabecera está configurado para aceptar conexiones de cualquier cliente en lugar de peering individual. El dispositivo de cabecera también se prueba sólo con claves previamente compartidas y 3DES y el algoritmo hash seguro (SHA) del procesador de servicios de extremo (ESP), código de autenticación de mensajes basado en hash (HMAC).



Configuraciones

En este documento, se utilizan estas configuraciones:

- Router 2600 de Cisco
- Dispositivo de cabecera IPSec - Router Cisco 3600
- Cisco 6160 DSLAM
- Procesador de ruta de nodo Cisco 6400 (NRP)

Tenga en cuenta estos puntos sobre las configuraciones:

- Se utiliza una clave previamente compartida. Para configurar las sesiones IPSec en varios peers, debe definir varias sentencias de definición de clave o debe configurar un mapa criptográfico dinámico. Si todas las sesiones comparten una única clave, debe utilizar una dirección de peer de 0.0.0.0.
- El conjunto de transformación se puede definir para ESP, Encabezado de autenticación (AH) o ambos para autenticación doble.
- Se debe definir al menos una definición de política de criptografía por peer. Los mapas criptográficos deciden el par que se utilizará para crear la sesión IPSec. La decisión se basa en la coincidencia de dirección definida en la lista de acceso. En este caso, es la lista de acceso 101.
- Los mapas criptográficos se deben definir tanto para las interfaces físicas (interfaz ATM 0/0 en este caso) como para la plantilla virtual.
- La configuración presentada en este documento trata solamente un túnel IPSec sobre una conexión DSL. Probablemente se necesiten funciones de seguridad adicionales para garantizar que su red no sea vulnerable. Estas funciones de seguridad pueden incluir listas de control de acceso (ACL) adicionales, traducción de direcciones de red (NAT) y el uso de un firewall con una unidad externa o un conjunto de funciones de firewall IOS. Cada una de estas funciones se puede utilizar para restringir el tráfico no IPSec hacia y desde el router.

Router 2600 de Cisco
`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
```

Dispositivo de cabecera IPSec - Router Cisco 3600

```
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
 !
```

Advertencias

Las conexiones ADSL se pueden configurar con una plantilla virtual o una interfaz de marcador.

Se utiliza una interfaz de marcador para configurar el CPE DSL para recibir una dirección del proveedor de servicios (la dirección IP se negocia). Una interfaz de plantilla virtual es una interfaz descendente y no admite la opción de dirección negociada, que es necesaria en el entorno DSL. Inicialmente se implementaron interfaces de plantilla virtual para entornos DSL. Actualmente, una interfaz de marcador es la configuración recomendada en el lado DSL CPE.

Se encuentran dos problemas en el momento de la configuración de las interfaces del marcador con IPSec:

- Id. de error de Cisco CSCdu30070 (sólo clientes registrados) —IPSec solo de software sobre DSL: brecha de cola de entrada en la interfaz del marcador DSL.
- Id. de error de Cisco CSCdu30335 (sólo clientes registrados) —IPSec basado en hardware sobre DSL: brecha de la cola de entrada en la interfaz del marcador.

La solución temporal actual para ambos problemas es configurar el CPE DSL con el uso de la interfaz de plantilla virtual como se describe en la configuración.

Las correcciones para ambos problemas se planifican para la versión 12.2(4)T del software del IOS de Cisco. Después de esta versión, se publica una versión actualizada de este documento para mostrar la configuración de la interfaz del marcador como otra opción.

Verificación

Esta sección proporciona la información que puede utilizar para confirmar que su configuración funciona correctamente.

Se pueden utilizar varios **comandos show** para verificar que la sesión IPSec se establece entre los pares. Los comandos son necesarios sólo en los pares IPSec, en este caso en las series 2600 y 3600 de Cisco.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show crypto engine connections active**: muestra cada SA de fase 2 generada y la cantidad de tráfico enviado.
- **show crypto ipsec sa** —Muestra IPSec SA generada entre peers.

Este es un ejemplo de resultado del comando **show crypto engine connections active**.

```
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
```

Este es un ejemplo de resultado del comando **show crypto ipsec sa**.

```
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:
```

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

El mensaje `"Modem state = 0x8"` que es informado por el comando **debug atm events** generalmente significa que WIC1-ADSL no puede recibir Carrier Detect desde el DSLAM conectado. En esta situación, el cliente necesita verificar que la señal DSL se suministra en los dos cables del medio en relación con el conector RJ11. Algunas compañías telefónicas proveen la señal DSL en los

dos pines externos en su lugar.

Comandos para Troubleshooting

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Antes de ejecutar **comandos debug**, consulte la Información Importante sobre Comandos Debug.

Precaución: No ejecute la depuración en una red en directo. El volumen de información que se muestra puede sobrecargar el router hasta el punto en que no se emiten flujos de datos ni mensajes CPUHOG.

- **debug crypto ipsec — Muestra eventos de IPSec.**
- **debug crypto isakmp — Muestra mensajes acerca de eventos IKE.**

Summary

La implementación de IPSec a través de una conexión ADSL proporciona una conexión de red segura y fiable entre las sucursales y los sitios centrales. El uso de las series 2600/3600 de Cisco con los módulos de cifrado de hardware y ADSL-WIC ofrece un menor coste de propiedad para el cliente, ya que ADSL e IPSec ahora se pueden lograr en una única solución de router. La configuración y las advertencias enumeradas en este documento deben servir como guía básica para configurar este tipo de conexión.

Información Relacionada

- Una Introducción al Cifrado de Seguridad IP (IPSec)
- Cisco 2600 Series Routers
- Redes privadas virtuales
- Soporte técnico de DSL y LRE
- Compatibilidad con productos de Universal Gateways
- Soporte de Tecnología de Discado y Acceso
- Soporte Técnico - Cisco Systems