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 un IPSec VPN típico. Vario el Acceso Remoto y conexiones del sitio a localizar están implicados entre las sucursales y los sitios centrales. Generalmente, los links WAN tradicionales tales como Frame Relay, el ISDN, y la marcación manual del módem son aprovisionado entre los sitios. Estas conexiones pueden implicar una tarifa de una sola vez costosa del aprovisionamiento y a los cargos mensuales costosos. También, para el ISDN y los usuarios de módem, puede haber tiempos de conexión largos.

El Asymmetric Digital Subscriber Line (ADSL) ofrece siempre-en, alternativa de bajo costo a estos links WAN tradicionales. Los datos encriptados del IPSec sobre un link ADSL ofrecen un seguro y una conexión confiable y guardan el dinero de los clientes. Un Customer Premises Equipment del ADSL tradicional (CPE) configurado en una sucursal requiere un módem ADSL que conecte con un dispositivo que origine y termine el tráfico IPSec. Esta figura muestra una red típica de ADSL.

Los Cisco 2600 y 3600 Router soportan el ADSL WAN Interface Card (WIC-1ADSL). Este WIC-

1ADSL es un multiservicios y una solución de acceso remoto diseñado para cubrir las necesidades de una sucursal. La introducción del WIC-1ADSL y de los módulos de encripción por hardware logra la demanda para el IPSec y el DSL en una sucursal en una solución del único router. El WIC-1ADSL elimina la necesidad de un módem DLS separado. El módulo de encripción por hardware proporciona hasta diez veces el funcionamiento sobre el cifrado software solamente mientras que descarga el cifrado ese los procesos del router.

Para más información sobre estos dos Productos, refiera a los ADSL WAN Interface Cards para el Cisco 1700, 2600, y los routeres de acceso modular y los módulos de red privada virtuales de las 3700 Series para el Cisco 1700, los 2600, los 3600, y las 3700 Series.

prerrequisitos

Requisitos

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 Router:

- Conjunto de características del Enterprise Plus 3DES del Software Release 12.1(5)YB de Cisco IOS®
- 64 MB DRAM para las Cisco 2600 Series, 96 MB DRAM para las Cisco 3600 Series
- 16 MB de destello para las Cisco 2600 Series, 32 MB de destello para las Cisco 3600 Series
- WIC-1 ADSL
- Módulos de encripción por hardwareAIM-VPN/BP y AIM-VPN/EP para las Cisco 2600 SeriesNM-VPN/MP para Cisco 3620/3640AIM-VPN/HP para el Cisco 3660

Cisco 6400 Series:

- Cisco IOS Software Release 12.1(5)DC1
- 64 MB DRAM
- 8 MB de destello

Cisco 6160 Series:

- Cisco IOS Software Release 12.1(7)DA2
- 64 MB DRAM
- 16 MB de destello

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Configurar

En esta sección, le presentan con la información que usted puede utilizar para configurar las características descritas en este documento.

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

Diagrama de la red

Este documento utiliza la configuración de la red mostrada este diagrama.

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

El Cisco 2600/3600 con el ADSL-WIC y el módulo de encripción por hardware entrena hasta el Cisco 6160 a un Digital Subscriber Line Access Multiplexer (DSLAM). El Cisco 6400 se utiliza como dispositivo de agrupamiento que termine a una sesión PPP que inicie del Cisco 2600 Router. El túnel IPsec origina en el CPE 2600 y termina en el Cisco 3600 en la oficina central, el dispositivo de cabecera del IPSec en este escenario. El dispositivo de cabecera se configura para validar las conexiones de cualquier cliente en vez de la conexión individual entre peers. El dispositivo de cabecera también se prueba con solamente las claves previamente compartidas y 3DES y el Edge Service Processor (ESP) - Secure Hash Algorithm (SHA) - el Hash-Based Message Authentication Code (HMAC).

Configuraciones

En este documento, se utilizan estas configuraciones:

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

Observe estas puntas sobre las configuraciones:

- Se utiliza una clave previamente compartida. Para configurar las sesiones del IPSec a los peeres múltiples, usted debe definir las declaraciones de definición clave múltiples o usted necesita configurar una correspondencia cifrada dinámica. Si todas las sesiones comparten una sola clave, usted debe utilizar a una dirección de peer de 0.0.0.0.
- El conjunto de la transformación se puede definir para el ESP, el Encabezado de autenticación, o ambos para la Autenticación doble.
- Por lo menos una definición de la política de criptografía se debe definir por el par. Las correspondencias de criptografía deciden al par para utilizar para crear sesión IPSec. La decisión se basa en la coincidencia del direccionamiento definida en la lista de acceso. En este caso, es access-list 101.
- Las correspondencias de criptografía se deben definir para las interfaces físicas (interfaz

ATM0/0 en este caso) y la virtual-plantilla.

- La configuración presentada en este documento discute solamente un túnel IPsec sobre una conexión DSL. Las características de seguridad complementaria son probablemente necesarias para asegurarse de que su red no es vulnerable. Estas funciones de seguridad pueden incluir el Listas de control de acceso (ACL) adicional, el Network Address Translation (NAT), y el uso de un Firewall con una unidad externa o un conjunto de características del escudo de protección IOS. Cada uno de estas características se puede utilizar para restringir el tráfico del no IPSec a 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 del IPSec - Cisco 3600 Router

```
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 virtual-plantilla o una interfaz del dialer.

Una interfaz del dialer se utiliza para configurar DSL CPE para recibir un direccionamiento del proveedor de servicio (se negocia la dirección IP). Una interfaz de plantilla virtual es una interfaz del down-down y no soporta la opción de la dirección negociada, que es necesaria en el entorno DSL. Las interfaces de plantilla virtual fueron implementadas inicialmente para los entornos DSL. Una interfaz del dialer es actualmente la configuración recomendada en DSL CPE el lateral.

Dos problemas se encuentran a la hora de la configuración de las interfaces del dialer con el IPSec:

- Id. de bug Cisco CSCdu30070 (clientes registrados solamente) — IPSec software solamente sobre el DSL: cuña de la cola de entrada en la interfaz del dialer DSL.
- Id. de bug Cisco CSCdu30335 (clientes registrados solamente) — IPSec basado en hardware sobre el DSL: cuña de la cola de entrada en la interfaz del dialer.

La solución alternativa actual para ambos problemas es configurar DSL CPE con el uso de la interfaz de plantilla virtual según lo descrito en la configuración.

Los arreglos para ambos problemas se planean para el Cisco IOS Software Release 12.2(4)T. Después de que esta versión, una versión actualizada de este documento se fije para mostrar la configuración de la interfaz del dialer como otra opción.

Verificación

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

Varios **comandos show** pueden ser utilizados para verificar que sesión IPSec está establecido entre los pares. Los comandos son necesarios solamente en los peeres IPSec, en este caso las Cisco y Series.

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 Fase 2 SA generada y la cantidad de tráfico enviado.
- **muestre IPSec crypto sa** — IPSec SA de las demostraciones construido entre los pares.

Ésta es salida del comando de ejemplo para el **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

Ésta es salida del comando de ejemplo para el **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:

Troubleshooting

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

El "estado del módem del = el mensaje 0x8" que es señalado por el **comando debug atm events** significa generalmente que el WIC1-ADSL no puede recibir la detección de la portadora del DSLAM conectado. En esta situación, las clientes necesitas de marcar que la señal DSL es aprovisionado en los dos alambres medios en relación con el conector RJ11. Algunas compañías telefónicas provision la señal DSL en los contactos del exterior dos en lugar de otro.

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 que usted publique los **comandos debug**, refiera a la información importante en los comandos Debug.

Precaución: No ejecute el debugging en una red en funcionamiento. El volumen de la información que visualiza puede sobrecargar a su router a la punta donde no se publica ningunos flujos de datos y mensajes Cpuhog Messages.

- debug crypto IPSec - Muestra eventos de IPSec.
- debug crypto Isakmp - muestra mensajes acerca de eventos IKE.

Resumen

La implementación del IPSec sobre una conexión ADSL proporciona un seguro y una conexión de red confiable entre las sucursales y los sitios centrales. El uso de la serie del Cisco 2600/3600 con el ADSL-WIC y los módulos de encripción por hardware ofrece el costo bajo de la propiedad al cliente mientras que ADSL y el IPSec se pueden ahora lograr en una solución del único router.

La configuración y las advertencias enumeradas en esta necesidad de papel de servir como pautas básicas configurar este tipo de conexión.

Información Relacionada

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