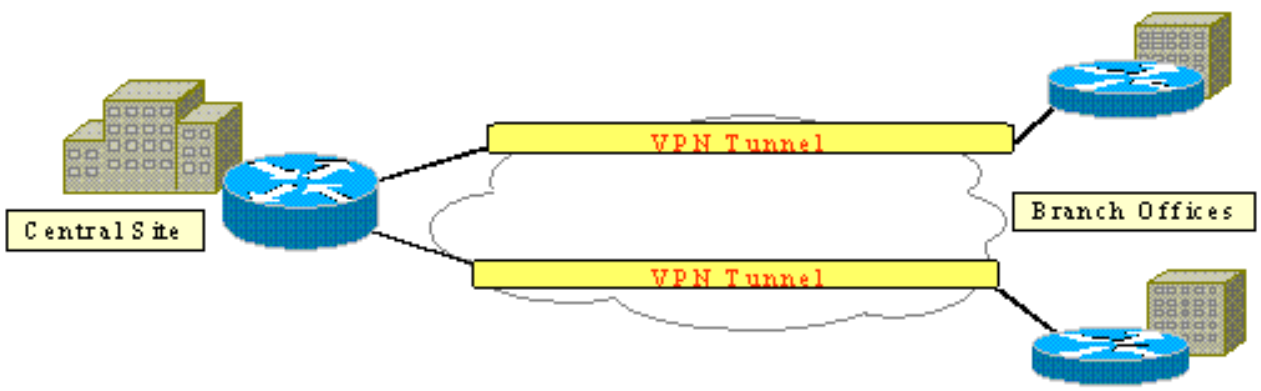
Configuração de IPSec sobre ADSL em um Cisco 2600/3600 com ADSL-WIC e módulos de criptografia de hardware

Contents

Introduction

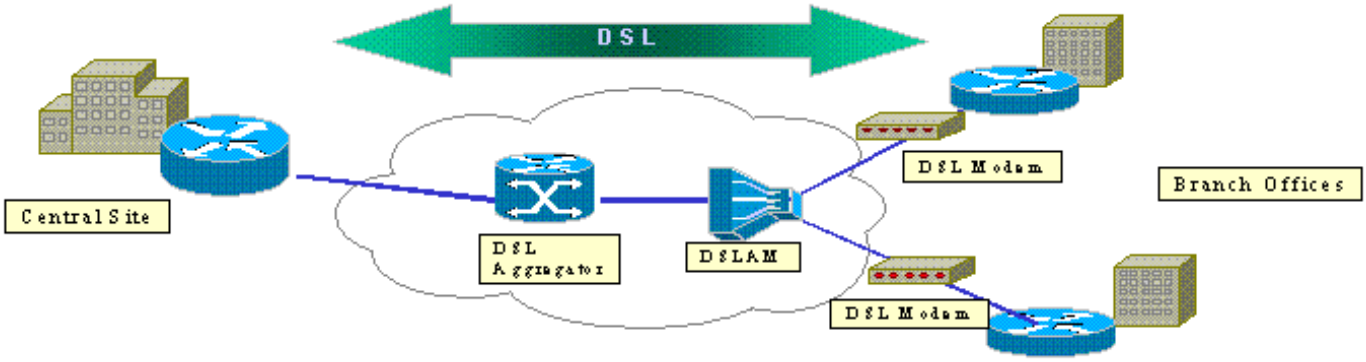
Com a expansão da Internet, os escritórios filiais exigem que suas conexões às instalações centrais sejam confiáveis e seguras. As Redes Privadas Virtuais (VPN) protegem as informações que são trafegadas pela Internet entre escritórios remotos e as instalações centrais. A Segurança IP (IPsec) pode ser usada para garantir que os dados que passam por essas VPN estejam criptografados. A criptografia propicia outra camada de segurança de rede.



Esta figura mostra uma VPN IPSec típica. Várias conexões de acesso remoto e de site para site

estão envolvidas entre filiais e locais centrais. Geralmente, os links de WAN tradicionais, como Frame Relay, ISDN e discagem de modem, são provisionados entre os sites. Essas conexões podem envolver uma taxa de provisionamento única cara e tarifas mensais caras. Além disso, para usuários de ISDN e modem, pode haver longos tempos de conexão.

A ADSL (Asymmetric Digital Subscriber Line) oferece uma alternativa sempre ativa e de baixo custo para esses links tradicionais de WAN. Os dados criptografados IPSec em um link ADSL oferecem uma conexão segura e confiável e economizam dinheiro dos clientes. Um equipamento tradicional nas instalações do cliente (CPE) ADSL instalado em uma filial requer um modem ADSL que se conecta a um dispositivo que origina e encerra o tráfego IPSec. Esta figura mostra uma rede ADSL típica.



Os roteadores Cisco 2600 e 3600 suportam a placa de interface WAN ADSL (WIC-1ADSL). Essa WIC-1ADSL é uma solução de acesso remoto e multisserviço projetada para atender às necessidades de uma filial. A introdução dos módulos de criptografia WIC-1ADSL e de hardware atende à demanda por IPSec e DSL em uma filial em uma única solução de roteador. A WIC-1ADSL elimina a necessidade de um modem DSL separado. O módulo de criptografia de hardware oferece até dez vezes mais desempenho do que a criptografia somente de software, já que descarrega a criptografia que processa do roteador.

Para obter mais informações sobre esses dois produtos, consulte ADSL WAN Interface Cards para os Cisco 1700, 2600 e 3700 Series Modular Access Routers e Virtual Private Network Modules para as séries Cisco 1700, 2600, 3600 e 3700 .

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

Roteadores Cisco 2600/3600 Series:

- Software Cisco IOS® versão 12.1(5)YB Enterprise PLUS 3DES Conjunto de recursos
- DRAM de 64 MB para a série Cisco 2600, DRAM de 96 MB para a série Cisco 3600

- Flash de 16 MB para a série Cisco 2600, Flash de 32 MB para a série Cisco 3600
- ADSL WIC-1
- Módulos de criptografia de hardwareAIM-VPN/BP e AIM-VPN/EP para a série Cisco 2600NM-VPN/MP para Cisco 3620/3640AIM-VPN/HP para Cisco 3660

Cisco 6400 Series:

- Software Cisco IOS versão 12.1(5)DC1
- DRAM 64 MB
- Flash 8 MB

Cisco 6160 Series:

- Software Cisco IOS versão 12.1(7)DA2
- DRAM 64 MB
- Flash de 16 MB

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você trabalhar em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Conventions

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

Configurar

Nesta seção, você verá as informações que podem ser usadas para configurar os recursos descritos neste documento.

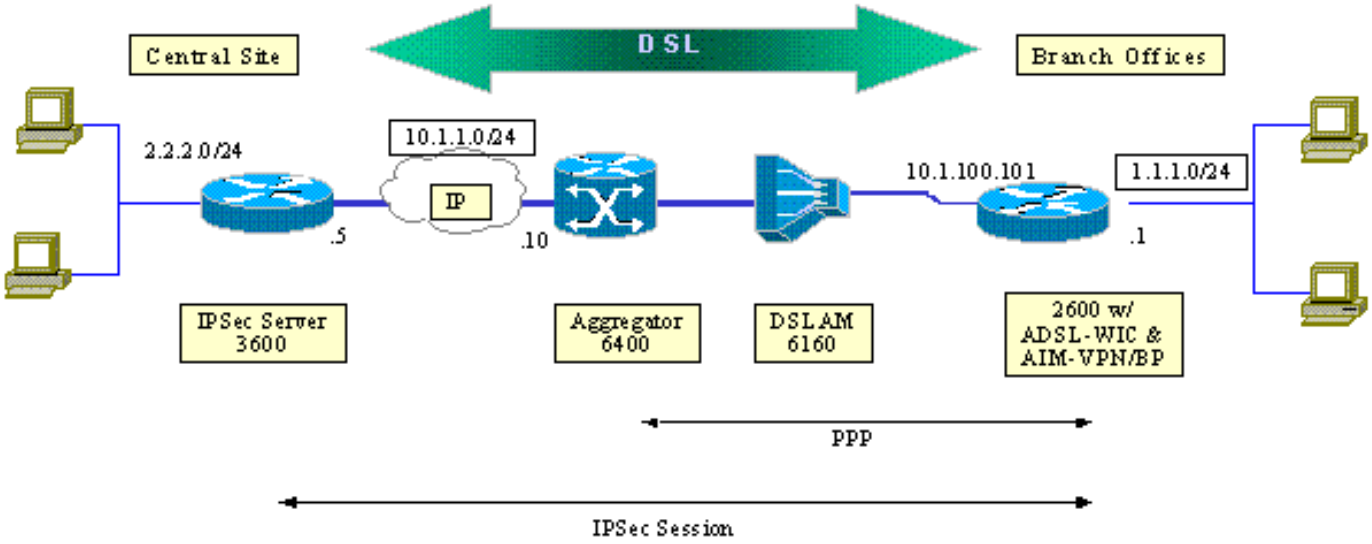
Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a Command Lookup Tool (somente clientes registrados) .

Diagrama de Rede

Este documento usa a configuração de rede mostrada neste diagrama.

Este teste simula uma conexão VPN IPSec que usa ADSL em um ambiente típico de filial.

O Cisco 2600/3600 com ADSL-WIC e módulo de criptografia de hardware treina até um Cisco 6160 Digital Subscriber Line Access Multiplexer (DSLAM). O Cisco 6400 é usado como um dispositivo de agregação que encerra uma sessão PPP que inicia a partir do roteador Cisco 2600. O túnel IPSec é originado no CPE 2600 e termina no Cisco 3600 no escritório central, o dispositivo headend IPSec neste cenário. O dispositivo headend é configurado para aceitar conexões de qualquer cliente em vez de peering individual. O dispositivo headend também é testado com apenas chaves pré-compartilhadas e o 3DES e o Edge Service Processor (ESP)-Secure Hash Algorithm (SHA)-Hash-based Message Authentication Code (HMAC).



Configurações

Este documento utiliza as seguintes configurações:

- Cisco 2600 Router
- Dispositivo headend IPSec - Roteador Cisco 3600
- DSLAM Cisco 6160
- Cisco 6400 Node Route Processor (NRP)

Observe estes pontos sobre as configurações:

- Uma chave pré-compartilhada é usada. Para configurar sessões de IPSec para vários peers, você deve definir várias instruções de definição de chave ou precisa configurar um mapa de criptografia dinâmico. Se todas as sessões compartilharem uma única chave, você deve usar um endereço de peer de 0.0.0.0.
- O conjunto de transformações pode ser definido para ESP, Authentication Header (AH) ou ambos para autenticação dupla.
- Pelo menos uma definição de política de criptografia deve ser definida por peer. Os mapas de criptografia decidem o peer a ser usado para criar a sessão IPSec. A decisão é baseada na correspondência de endereço definida na lista de acesso. Nesse caso, é access-list 101.
- Os mapas de criptografia devem ser definidos para as interfaces físicas (interface ATM 0/0 neste caso) e para o modelo virtual.
- A configuração apresentada neste documento discute somente um túnel IPSec sobre uma conexão DSL. Provavelmente, são necessários recursos de segurança adicionais para garantir que sua rede não esteja vulnerável. Esses recursos de segurança podem incluir listas de controle de acesso (ACLs) adicionais, conversão de endereço de rede (NAT) e o uso de um firewall com uma unidade externa ou um conjunto de recursos de firewall do IOS. Cada um desses recursos pode ser usado para restringir o tráfego não IPSec de e para o roteador.

Cisco 2600 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 10.1.1.5 ! 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 headend IPSec - Roteador 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
```

DSLAM Cisco 6160

```
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.

 !
```

NRP do Cisco 6400

```
!
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
!
```

Caveats

As conexões ADSL podem ser configuradas com um modelo virtual ou uma interface de discador.

Uma interface de discador é usada para configurar o CPE DSL para receber um endereço do provedor de serviços (o endereço IP é negociado). Uma interface de modelo virtual é uma interface inativa e não suporta a opção de endereço negociado, que é necessária no ambiente DSL. As interfaces de modelo virtual foram inicialmente implementadas para ambientes DSL. Atualmente, uma interface de discador é a configuração recomendada no lado DSL CPE.

Dois problemas são encontrados no momento da configuração de interfaces de discador com IPSec:

- ID de bug da Cisco CSCdu30070 (somente clientes registrados) — IPSec somente de software sobre DSL: input queue wedge na interface do discador DSL.
- ID de bug da Cisco CSCdu30335 (somente clientes registrados) — IPSec baseado em hardware sobre DSL: input queue wedge na interface do discador.

A solução atual para ambos os problemas é configurar o CPE DSL com o uso da interface de modelo virtual conforme descrito na configuração.

Correções para ambos os problemas estão planejadas para o Cisco IOS Software Release 12.2(4)T. Após esta versão, uma versão atualizada deste documento é publicada para mostrar a configuração da interface do discador como outra opção.

Verificar

Esta seção fornece as informações que você pode usar para confirmar se sua configuração funciona corretamente.

Vários comandos **show** podem ser usados para verificar se a sessão IPSec está estabelecida entre os pares. Os comandos são necessários apenas nos pares IPSec, neste caso, nas séries Cisco 2600 e 3600.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show crypto engine connections ative** —Mostra cada SA da Fase 2 criado e a quantidade de tráfego enviado.
- **show crypto ipsec sa** —Mostra SA IPSec criada entre pares.

Este é um exemplo de saída do comando **show crypto engine connections ative**.

```
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 é um exemplo de saída do 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 seção fornece as informações que você pode usar para solucionar problemas de sua configuração.

A mensagem `"Modem state = 0x8"` que é reportada pelo comando **debug atm events** geralmente significa que o WIC1-ADSL não pode receber Carrier Detect do DSLAM conectado. Nessa situação, o cliente precisa verificar se o sinal DSL é fornecido nos dois fios do meio em relação ao conector RJ11. Em vez disso, alguns Telcos provisionam o sinal DSL nos dois pinos externos.

Comandos de solução de problemas

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Observação: antes de emitir comandos **debug**, consulte Informações importantes sobre comandos debug.

Cuidado: não execute a depuração em uma rede ativa. O volume de informações exibidas pode sobrecarregar o roteador até o ponto em que nenhum fluxo de dados e mensagem CPUHOG são emitidos.

- **debug crypto ipsec** — Exibe eventos de IPSec.
- **debug crypto isakmp — Exibe mensagens sobre eventos de IKE.**

Summary

A implementação de IPSec em uma conexão ADSL fornece uma conexão de rede segura e confiável entre filiais e locais centrais. O uso da série Cisco 2600/3600 com os módulos de criptografia ADSL-WIC e de hardware oferece um menor custo de propriedade para o cliente, já que o ADSL e o IPSec agora podem ser realizados em uma única solução de roteador. A configuração e as advertências listadas neste documento precisam servir como orientação básica para configurar esse tipo de conexão.

Informações Relacionadas

- Uma introdução à criptografia do protocolo de segurança IP (IPSEC)
- Cisco 2600 Series Routers
- Redes Privadas Virtuais
- Suporte técnico DSL e LRE
- Suporte a produtos de gateways universais
- Suporte à tecnologia de discagem e acesso
- Suporte Técnico - Cisco Systems