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

Índice

Introdução

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 um IPSec VPN típico. Um número Acesso remoto e de conexões da site para site são involvidos entre escritórios filiais e instalações central. Geralmente, o WAN tradicional liga como o Frame Relay, ISDN, e o modem dialup é fornecida entre os locais. Estas conexões podem envolver uma único taxa cara do abastecimento e umas cobranças mensais caras. Também, para o ISDN e os usuários de modem, pode haver uns tempos de conexão longos.

O Asymmetric Digital Subscriber Line (ADSL) oferece sempre-em, alternativa de custo baixo a estes links do WAN tradicional. Os dados criptografados do IPsec sobre um link ADSL oferecem um seguro e uma conexão confiável e salvar o dinheiro dos clientes. Um Customer Premises Equipment do ADSL tradicional (CPE) estabelecido em um escritório filial exige um modem de ADSL que conecte a um dispositivo que origine e termine o tráfego de IPSec. Esta figura mostra uma rede ADSL típica.

Os Cisco 2600 e 3600 Router apoiam a placa de interface WAN ADSL (WIC-1ADSL). Este WIC-

1ADSL é um multi-serviço e uma solução de acesso remoto projetados encontrar as necessidades de um escritório filial. A introdução do WIC-1ADSL e dos módulos de criptografia de hardware realiza a procura para o IPsec e o DSL em um escritório filial em uma solução do roteador único. O WIC-1ADSL elimina a necessidade para um modem DSL separado. O módulo de criptografia de hardware fornece até dez vezes o desempenho sobre a criptografia somente software enquanto offloads a criptografia essa processos do roteador.

Para obter mais informações sobre deste dois Produtos, refira placas de interface WAN ADSL para o Cisco 1700, 2600, e Roteadores e módulos de rede privada virtuais do acesso modular do 3700 Series para o Cisco 1700, os 2600, os 3600, e o 3700 Series.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Cisco 2600/3600 Series Router:

- Conjunto de recursos do Enterprise Plus 3DES do Software Release 12.1(5)YB de Cisco IOS®
- 64 MB DRAM para o Cisco 2600 Series, 96 MB DRAM para o Cisco 3600 Series
- 16 MB instantâneo para o Cisco 2600 Series, 32 MB instantâneo para o Cisco 3600 Series
- ADSL WIC-1
- Módulos de criptografia de hardwareAIM-VPN/BP e AIM-VPN/EP para o Cisco 2600 SeriesNM-VPN/MP para Cisco 3620/3640AIM-VPN/HP para o Cisco 3660

Cisco 6400 Series:

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

Cisco 6160 Series:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você trabalhar em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar

Nesta seção, você é presentado com a informação que você pode se usar para configurar as características descritas neste documento.

Note: 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 instalação de rede mostrada este diagrama.

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

O Cisco 2600/3600 com o ADSL-WIC e o módulo de criptografia de hardware treina até o Cisco 6160 um multiplexador de acesso de linha de assinante digital (DSLAM). O Cisco 6400 é usado como um dispositivo de agregação que termine uma sessão de PPP que inicie do Cisco 2600 Router. O túnel de IPsec origina no CPE 2600 e termina no Cisco 3600 no escritório central, o dispositivo de fim de cabeçalho do IPsec nesta encenação. O dispositivo de fim de cabeçalho é configurado para aceitar conexões de todo o cliente em vez do peering individual. O dispositivo de fim de cabeçalho é testado igualmente com somente chaves pré-compartilhada e 3DES e Edge Service Processor (ESP) - Secure Hash Algorithm (SHA) - o Hash-Based Message Authentication Code (HMAC).

Configurações

Este documento utiliza as seguintes configurações:

- Cisco 2600 Router
- Dispositivo de fim de cabeçalho do IPsec - Cisco 3600 Router
- Cisco 6160 DSLAM
- Cisco 6400 Node Route Processor (NRP)

Note estes pontos sobre as configurações:

- Uma chave pré-compartilhada é usada. A fim estabelecer sessões IPSec aos peer múltiplos, você deve definir indicações definição-chaves múltiplas ou você precisa de configurar um mapa cripto dinâmico. Se todas as sessões compartilham de uma única chave, você deve usar um endereço de peer de 0.0.0.0.
- O grupo da transformação pode ser definido para o ESP, o Authentication Header (AH), ou ambos para a Autenticação dupla.
- Pelo menos uma definição da política de criptografia deve ser definida pelo par. Os crypto map decidem o par usar-se para criar a sessão IPSec. A decisão é baseada no fósforo do endereço definido na lista de acessos. Nesta instância, é access-list 101.
- Os crypto map devem ser definidos para as interfaces física (relação ATM0/0 neste caso) e o virtual-molde.
- A configuração apresentada neste documento discute somente um túnel de IPsec sobre uma conexão DSL. As características de segurança adicional são precisadas provavelmente a fim assegurar-se de que sua rede não seja vulnerável. Estes recursos de segurança podem incluir o Access Control Lists (ACLs) adicional, o Network Address Translation (NAT), e o uso

de um Firewall com uma unidade externa ou um conjunto de recursos do firewall de IOS. Cada um destas características pode ser usada a fim restringir o tráfego não-IPSec a e do 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 de fim de cabeçalho do 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

```
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.

 !
```

Caveats

As conexões ADSL podem ser configuradas com um virtual-molde ou uma interface do discador.

Uma interface do discador é usada a fim configurar o DSL CPE para receber um endereço do provedor de serviços (o endereço IP de Um ou Mais Servidores Cisco ICM NT é negociado). Uma interface de molde virtual é uma relação do down-down e não apoia a opção do endereço negociável, que é necessária no ambiente DSL. As interfaces de molde virtual foram executadas inicialmente para ambientes DSL. Atualmente uma interface do discador é a configuração recomendada no lado do DSL CPE.

Duas edições são encontradas na altura da configuração das interfaces do discador com o IPsec:

- Identificação de bug Cisco CSCdu30070 (clientes registrados somente) — IPsec somente software sobre o DSL: cunha da fila de entrada na interface do discador DSL.
- Identificação de bug Cisco CSCdu30335 (clientes registrados somente) — IPsec com base em hardware sobre o DSL: cunha da fila de entrada na interface do discador.

A solução alternativa atual para both of these edições é configurar o DSL CPE com o uso da interface de molde virtual como descrito na configuração.

Os reparos para both of these edições são planejados para o Cisco IOS Software Release 12.2(4)T. Depois que esta liberação, uma versão actualizado deste documento é afixada a fim mostrar a configuração da interface do discador como uma outra opção.

Verificar

Esta seção fornece a informação que você pode se usar a fim confirmar que sua configuração trabalha corretamente.

Diversos **comandos show** podem ser usados a fim verificar que a sessão IPSec está estabelecida entre os pares. Os comandos são necessários somente nos ipsec peer, neste caso o Cisco e Series.

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 active – Mostra cada fase 2 SA embutida e a quantidade de tráfego enviado.
- **mostre IPsec cripto sa** — IPsec SA das mostras construído entre pares.

Este é exemplo de saída de comando para o **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 exemplo de saída de comando para o **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 seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

O “estado do modem = a mensagem de 0x8" que é relatada pelo **comando debug atm events** significa geralmente que o WIC1-ADSL é incapaz de receber a revelação do sinal de comunicação do DSLAM conectado. Nesta situação, as necessidades de cliente de certificar-se do sinal DSL seja fornecida nos dois fios médios relativo ao conector RJ11. Alguns telcos provision o sinal DSL nos pinos da parte externa dois pelo contrário.

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.

Note: Antes que você emita **comandos debug**, refira a informação importante em comandos Debug.

Caution: Não execute a eliminação de erros em uma rede viva. O volume de informação que indica pode sobrecarregar seu roteador ao ponto onde nenhuns fluxo de dados e mensagem Cpuhog Messages são emitidos.

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

Resumo

A aplicação do IPsec sobre uma conexão ADSL fornece um seguro e uma conexão de rede confiável entre escritórios filiais e instalações central. O uso da série do Cisco 2600/3600 com o ADSL-WIC e os módulos de criptografia de hardware oferece custos mais baixos da posse ao cliente enquanto o ADSL e o IPsec podem agora ser realizados em uma solução do roteador único. A configuração e as advertências alistadas nesta necessidade de papel de servir como uma diretriz básica para estabelecer este tipo de conexão.

Informações Relacionadas

- Uma introdução à criptografia do protocolo de segurança IP (IPSEC)
- Cisco 2600 Series Routers
- Redes privadas virtuais
- Suporte técnico do DSL e LRE
- Apoio de Produtos do Universal Gateways
- Suporte por tecnologia do Discar e acessar
- Suporte Técnico - Cisco Systems