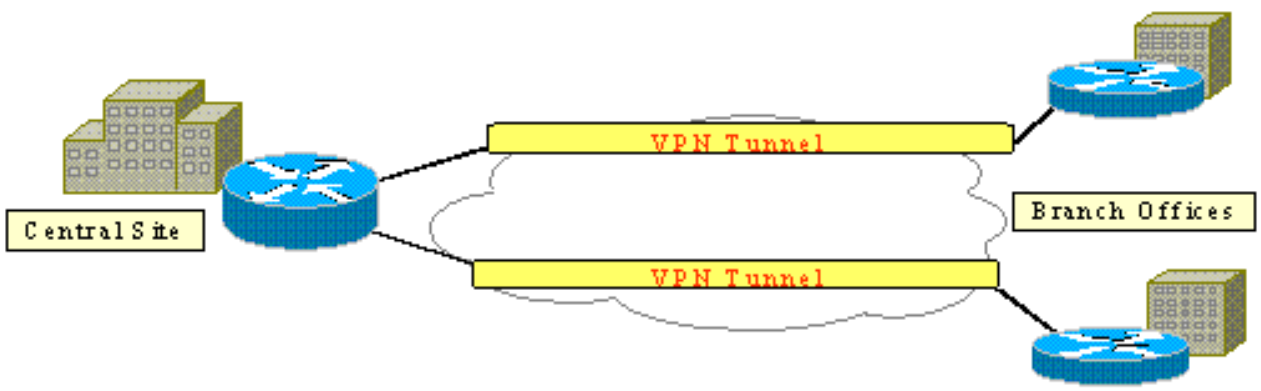
IPsec over ADSL configureren op een Cisco 2600/3600 met ADSL-WIC- en hardwareencryptie-modules

Inhoud

Inleiding

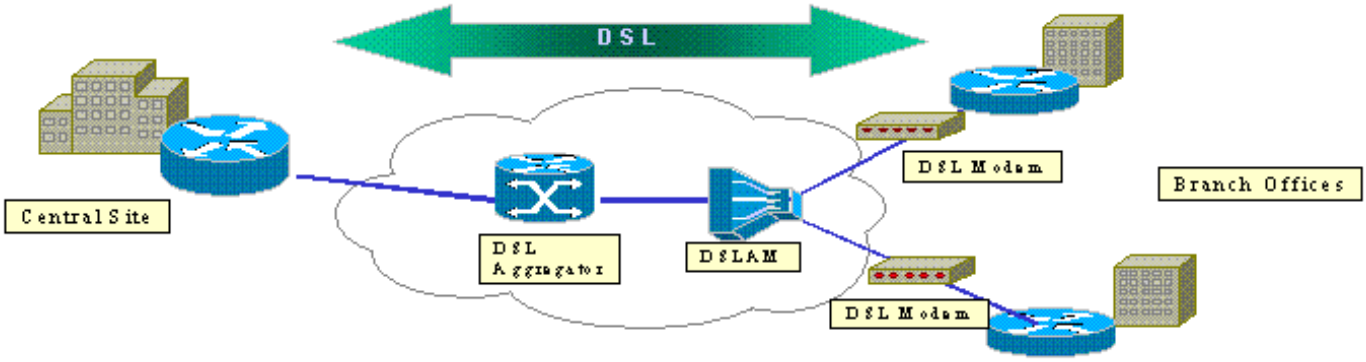
Als het internet zich uitbreidt, eisen bijkantoren dat hun verbindingen met centrale sites betrouwbaar en veilig zijn. Virtual Private Networks (VPN's) beschermen informatie tussen externe vestigingen en centrale sites wanneer deze over het internet reist. IP Security (IPSec) kan worden gebruikt om te waarborgen dat de gegevens die over deze VPN's passeren, zijn versleuteld. De encryptie verstrekt een andere laag van netwerkveiligheid.



Dit getal is een standaard IPSec VPN. Een aantal externe toegang en site-to-site verbindingen zijn

betrokken tussen filialen en centrale locaties. Normaal gesproken worden de traditionele WAN-koppelingen zoals Frame Relay, ISDN en modemdialup tussen de sites provisioneerd. Deze verbindingen kunnen een dure eenmalige provisioningvergoeding en dure maandelijkse kosten met zich meebrengen. Ook voor ISDN- en modemgebruikers kunnen er lange verbindingstijden zijn.

Asymmetric Digital Subscriber Line (ADSL) biedt een altijd-on, goedkoop alternatief voor deze traditionele WAN-links. Gecodeerde IPSec-gegevens via een ADSL-link bieden een beveiligde en betrouwbare verbinding en bespaart klanten geld. Een traditionele CPE (ADSL) die in een bijkantoor wordt geïnstalleerd vereist een ADSL-modem die op een apparaat wordt aangesloten dat van oorsprong en beëindiging IPSec-verkeer is. Dit getal is een typisch ADSL-netwerk.



De routers van Cisco 2600 en 3600 ondersteunen de WAN-interfacekaart met ADSL (WIC-1 ADSL). Deze WIC-1ADSL is een multiservice- en afstandstoegangsoplossing die is ontworpen om aan de behoeften van een bijkantoor te voldoen. De introductie van de WIC-1ADSL- en hardwareencryptiemodules bereikt de vraag naar IPSec en DSL in een bijkantoor in één enkele routeroplossing. WIC-1ADSL heft de noodzaak van een afzonderlijke DSL-modem op. De hardware encryptie module biedt tot tien keer de prestaties via software-only encryptie terwijl het de encryptie die van de router verwerkt ontkoppelt.

Raadpleeg voor meer informatie over deze twee producten WAN-interfacekaarten met ADSL voor Cisco 1700, 2600 en 3700 Series modulaire toegangsrouters en Virtual Private Network modules voor Cisco 1700, 2600, 3600 en 3700 Series .

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

Cisco 2600/3600 Series routers:

- Cisco IOS®-softwarerelease 12.1(5)YB Enterprise PLUS 3DES-functieset
- DRAM 64 MB voor Cisco 2600 Series, DRAM 96 MB voor de Cisco 3600-serie

- Flash 16 MB voor Cisco 2600 Series, Flash 32 MB voor Cisco 3600 Series
- WIC-1 ADSL
- Hardware encryptie-modulesAIM-VPN/BP en AIM-VPN/EP voor Cisco 2600 Series IPNM-VPN/MP voor Cisco 3620/3640AIM-VPN/HP voor Cisco 3660

Cisco 6400 Series:

- Cisco IOS-softwarerelease 12.1(5)DC1
- DRAM 64 MB
- Flitser 8 MB

Cisco 6160 Series:

- Cisco IOS-softwarerelease 12.1(7)DA2
- DRAM 64 MB
- Flitser 16 MB

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de mogelijke impact van een opdracht begrijpt voordat u het gebruikt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren

In deze sectie wordt u gepresenteerd met de informatie die u kunt gebruiken om de functies te configureren die in dit document worden beschreven.

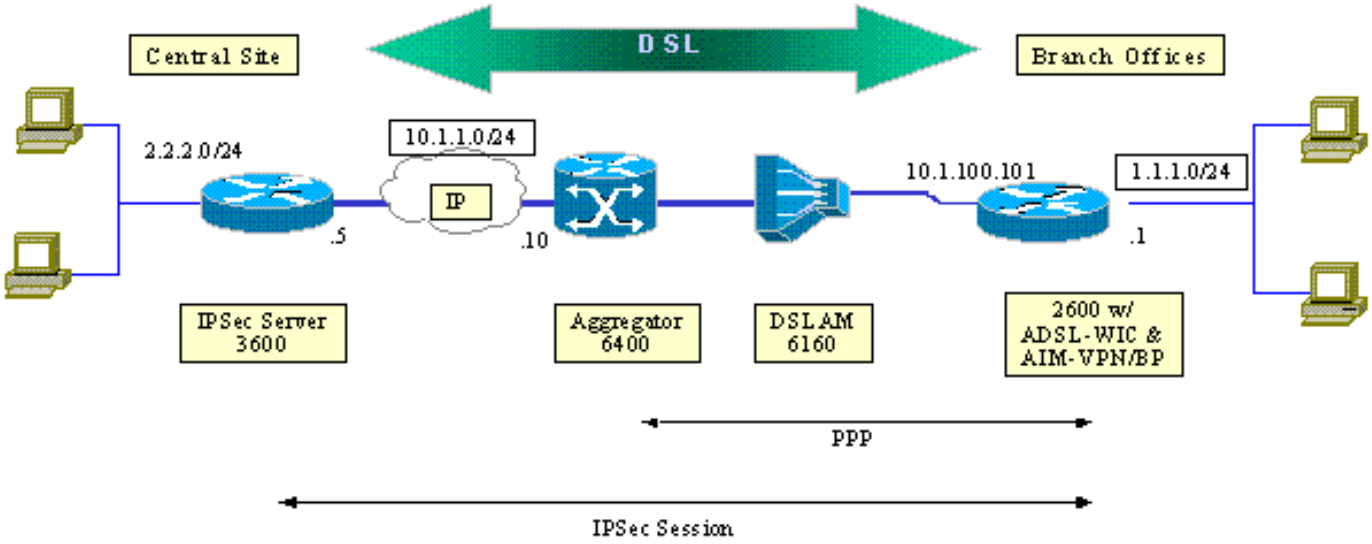
N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit schema zijn weergegeven.

Deze test simuleert een verbinding van IPSec VPN die ADSL in een typische omgeving van het bijkantoor gebruikt.

Cisco 2600/3600 met de ADSL-WIC- en hardwareencryptie-module treint naar een Cisco 6160 Digital Subscriber Line Multiplexer (DSLAM). Cisco 6400 wordt gebruikt als een aggregatiemiddel dat een PPP-sessie beëindigt die van Cisco 2600 router initieert. De IPSec-tunnel komt voort uit CPE 2600 en eindigt bij Cisco 3600 in het centrale bureau, het head-end apparaat van IPSec in dit scenario. Het head-end apparaat is ingesteld om verbindingen van een willekeurige client te accepteren in plaats van een individuele gebruiker. Het head-end apparaat wordt ook getest met alleen vooraf gedeelde toetsen en 3DES en Edge Service Processor (ESP)-Secure Hash Algorithm (SHA)-Hash-Based Message Verifier Code (HMAC).



Configuraties

Dit document gebruikt deze configuraties:

- Cisco 2600 router
- IPSec Head-end apparaat - Cisco 3600 router
- Cisco 6160 DSLAM
- Cisco 6400 routeprocessor voor knooppunt (NRP)

Let op deze punten over de configuraties:

- Er wordt een vooraf gedeelde toets gebruikt. Om IPSec sessies aan meerdere peers op te stellen moet u meerdere zeer belangrijke definitieverklaringen definiëren of u moet een dynamische crypto kaart vormen. Als alle sessies één enkele sleutel delen, moet u een peer adres van 0.0.0 gebruiken.
- De transformatieset kan worden gedefinieerd voor ESP, Verificatieheader (AH) of beide voor dubbele verificatie.
- Ten minste één cryptobeleidsdefinitie moet per peer worden gedefinieerd. De crypto kaarten beslissen de peer om te gebruiken om de IPSec zitting te creëren. De beslissing is gebaseerd op de adresmatch die in de toegangslijst is gedefinieerd. In dit geval is het toegangslijst 101.
- De crypto-kaarten moeten worden gedefinieerd voor zowel de fysieke interfaces (in dit geval interface ATM 0/0) als de virtuele sjabloon.
- De configuratie die in dit document wordt gepresenteerd, bespreekt alleen een IPSec-tunnel via een DSL-verbinding. Aanvullende beveiligingsfuncties zijn waarschijnlijk nodig om te voorkomen dat uw netwerk kwetsbaar is. Deze beveiligingsfuncties kunnen aanvullende toegangscontrolelijsten (ACL's), netwerkadresomzetting (NAT) en het gebruik van een firewall met een externe eenheid of een IOS-firewallfunctieset omvatten. Elk van deze functies kan worden gebruikt om niet-IPSec-verkeer naar en van de router te beperken.

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
```

IPSec Head-end apparaat - 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
```

```
!
```

Caveats

U kunt de ADSL-verbindingen configureren met een virtuele sjabloon of een dialerinterface.

Een dialerinterface wordt gebruikt om DSL CPE te configureren om een adres van de dienstverlener te ontvangen (IP-adres wordt onderhandeld). Een virtuele-sjabloon interface is een down-interface en ondersteunt de overeengekomen adresoptie niet, die in de DSL-omgeving nodig is. Virtuele sjablooninterfaces werden aanvankelijk geïmplementeerd voor DSL-omgevingen. Momenteel is een dialerinterface de aanbevolen configuratie aan de CPE-kant van DSL.

Ten tijde van de configuratie van de dialerinterfaces met IPSec worden twee problemen gevonden:

- Cisco bug-ID CSCdu30070 (alleen geregistreerde klanten) — IPSec-over-DSL: kleurendraaier op DSL-dialerinterface.
- Cisco bug-ID CSCdu30335 (alleen geregistreerde klanten) — op hardware gebaseerde IPSec over DSL: kleurendruk op de invoerwachtrij op dialer interface.

De huidige workround voor beide kwesties is om de DSL CPE met het gebruik van de virtuele-sjabloon interface te configureren zoals in de configuratie beschreven wordt.

Er zijn oplossingen voor beide problemen gepland voor Cisco IOS-softwarerelease 12.2(4)T. Na deze release wordt een aangepaste versie van dit document gepost om de configuratie van de dialer-interface als een andere optie te tonen.

Verifiëren

Deze sectie verschaft de informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Er kunnen verschillende opdrachten worden gebruikt om te controleren of de IPSec-sessie tussen de peers is ingesteld. De opdrachten zijn alleen nodig op de IPSec-peers, in dit geval de Cisco 2600 en 3600-serie.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

- **tonen de crypto motor verbindingen actief** - toont elke gebouwde fase 2 SA en de hoeveelheid verstuurd verkeer.
- **toon crypto ipsec sa**-Toont IPSec SA gebouwd tussen peers.

Dit is steekproefuitvoer voor de **actieve** opdracht van de **sleutelcrypto-motorverbindingen**.

```
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
```

Dit is een voorbeeldopdracht uitvoer voor de **show crypto ipsec als** opdracht.

```
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:
```

Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Het `"Modem state = 0x8"` bericht dat door de opdracht **debug ATM** gebeurtenissen wordt gemeld betekent meestal dat WIC1-ADSL niet Carrier Detect van de aangesloten DSLAM kan ontvangen. In deze situatie moet de klant controleren dat het DSL-signaal voorzien is van de middentwee bedradingen ten opzichte van de RJ11-connector. Sommige telcos voorzien in het DSL-signaal op

de buitenkant twee spelden in plaats daarvan.

Opdrachten voor probleemoplossing

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Opmerking: Voordat u **debug-**opdrachten afgeeft, raadpleegt u de belangrijke informatie over debug-opdrachten.

Waarschuwing: wijden niet aan het fouilleren op een levend netwerk. Het volume van informatie dat toont uw router kan overladen tot het punt waar geen gegevensstromen en CPUHOG berichten worden uitgegeven.

- **debug van crypto IPSec**-displays IPSec-gebeurtenissen.
- **debug crypto Isakmp**-displays over IKE gebeurtenissen.

Samenvatting

Implementatie van IPSec via een ADSL-verbinding biedt een veilige en betrouwbare netwerkverbinding tussen filialen en centrale locaties. Het gebruik van de Cisco 2600/3600-serie met de ADSL-WIC- en hardwareencryptiemodules biedt de klant lagere eigendomskosten aangezien ADSL en IPSec nu in één routeroplossing kunnen worden verwezenlijkt. De configuratie en voorbehouden die in dit document worden genoemd, moeten dienen als een richtsnoer voor het opzetten van dit type verbindingen.

Gerelateerde informatie

- Een Inleiding aan IP Security (IPSec) encryptie
- Cisco 2600 Series routers
- Virtual Private Networks
- Technische ondersteuning voor DSL en LRE
- Ondersteuning voor universele gateways
- Ondersteuning van inbel- en toegangstechnologie
- Technische ondersteuning - Cisco-systemen