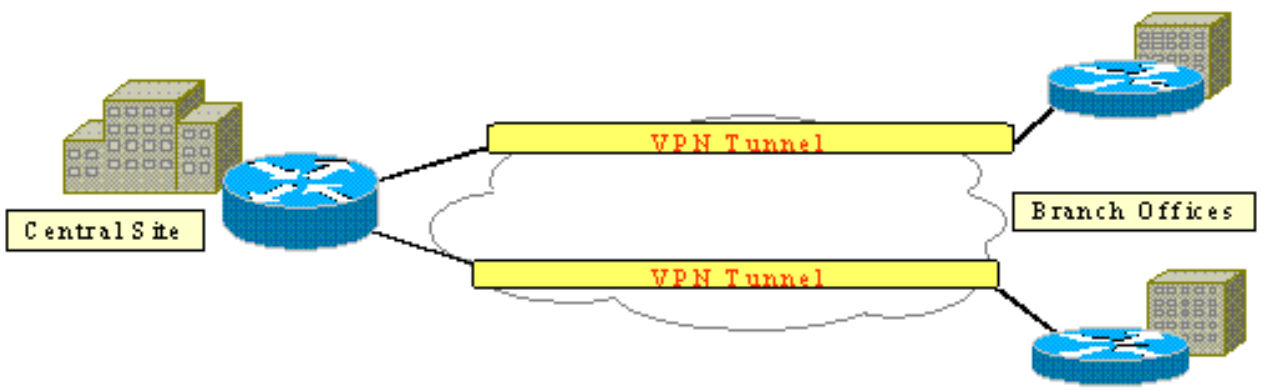
Configurazione di IPSec over ADSL su uno switch Cisco 2600/3600 con ADSL-WIC e moduli di crittografia hardware

Sommario

Introduzione

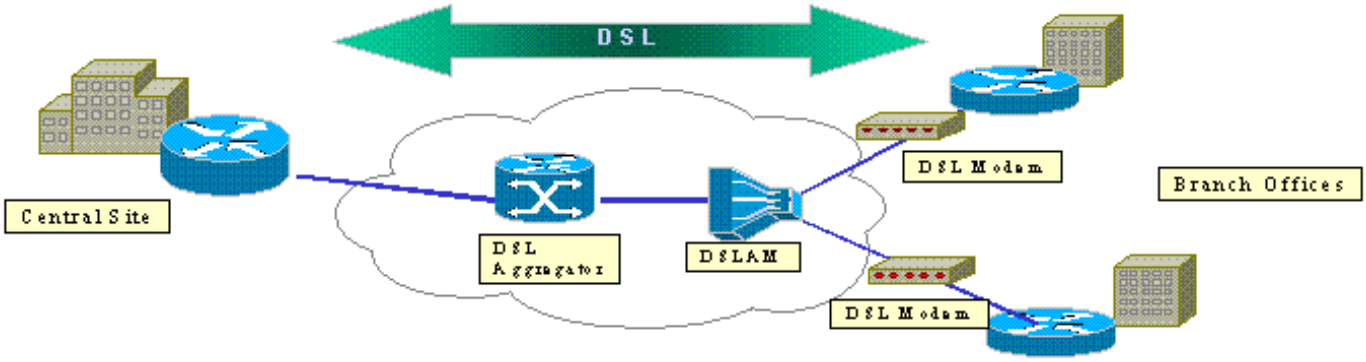
Con l'espansione di Internet, le filiali richiedono connessioni a siti centrali affidabili e sicure. Le VPN (Virtual Private Network) proteggono le informazioni tra uffici remoti e siti centrali durante il loro trasferimento su Internet. IP Security (IPSec) può essere utilizzato per garantire che i dati che passano attraverso queste VPN siano crittografati. La crittografia fornisce un altro livello di protezione di rete.



Nella figura viene illustrata una VPN IPSec tipica. Tra le filiali e i siti centrali sono coinvolte

numerose connessioni di accesso remoto e da sito a sito. In genere, i collegamenti WAN tradizionali, ad esempio Frame Relay, ISDN e la connessione remota via modem, vengono forniti tra i siti. Queste connessioni possono comportare costi di provisioning una tantum e costi mensili elevati. Inoltre, per gli utenti ISDN e modem, i tempi di connessione possono essere lunghi.

L'ADSL (Asymmetric Digital Subscriber Line) offre un'alternativa sempre attiva e a basso costo a questi collegamenti WAN tradizionali. I dati crittografati IPSec su un collegamento ADSL offrono una connessione sicura e affidabile e consentono di risparmiare sui costi. Le apparecchiature CPE (Customer Premise Equipment) ADSL tradizionali installate in una succursale di un ufficio richiedono un modem ADSL che si connetta a un dispositivo che origina e termina il traffico IPSec. Nella figura viene illustrata una tipica rete ADSL.



I router Cisco 2600 e 3600 supportano la scheda di interfaccia WAN ADSL (WIC-1ADSL). WIC-1ADSL è una soluzione di accesso remoto e multiservizio progettata per soddisfare le esigenze delle filiali. L'introduzione dei moduli ADSL e di crittografia hardware WIC-1 soddisfa la domanda di IPSec e DSL in una succursale di un ufficio in una soluzione a router singolo. WIC-1ADSL elimina la necessità di un modem DSL separato. Il modulo di crittografia hardware offre prestazioni fino a dieci volte superiori rispetto alla crittografia solo software in quanto scarica la crittografia elaborata dal router.

Per ulteriori informazioni su questi due prodotti, fare riferimento alle schede di interfaccia WAN ADSL per i Cisco serie 1700, 2600 e 3700 Modular Access Router e Virtual Private Network Module per i Cisco serie 1700, 2600, 3600 e 3700.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Cisco serie 2600/3600 Router:

- Software Cisco IOS® versione 12.1(5)YB Enterprise PLUS 3DES - Set funzioni

- DRAM da 64 MB per Cisco serie 2600, DRAM da 96 MB per Cisco serie 3600
- Flash 16 MB per Cisco serie 2600, Flash 32 MB per Cisco serie 3600
- ADSL WIC-1
- Moduli di crittografia hardwareAIM-VPN/BP e AIM-VPN/EP per Cisco serie 2600NM-VPN/MP per Cisco 3620/3640AIM-VPN/HP per Cisco 3660

Cisco serie 6400:

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

Cisco serie 6160:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

In questa sezione vengono presentate le informazioni che è possibile utilizzare per configurare le funzionalità descritte più avanti nel documento.

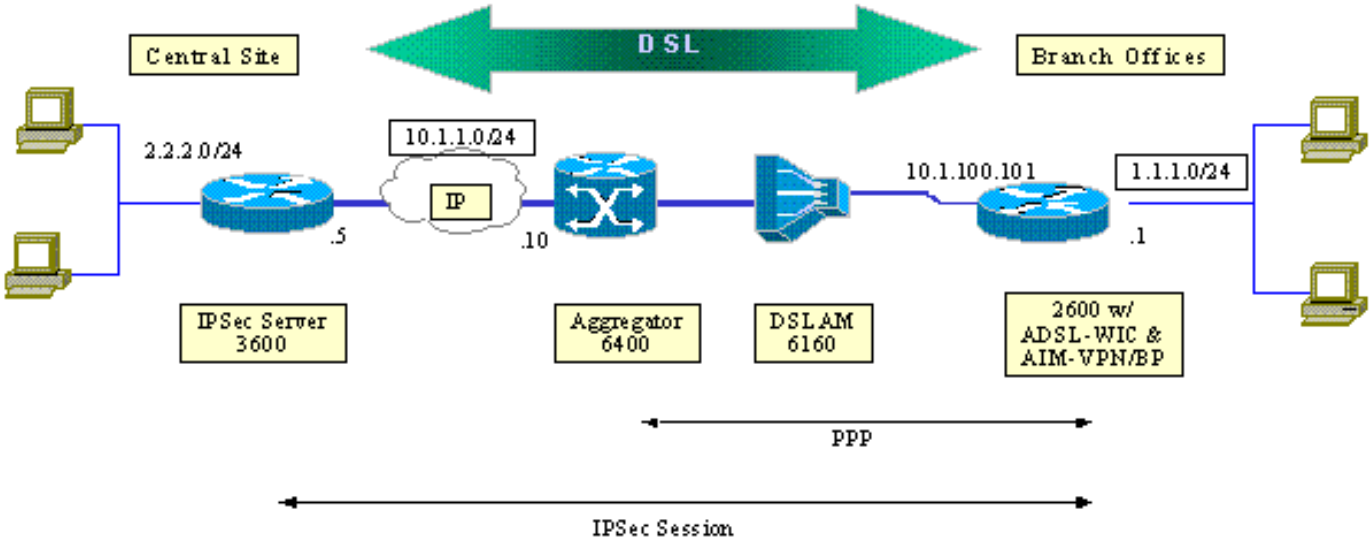
Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.

Questo test simula una connessione VPN IPSec che utilizza ADSL in un tipico ambiente di filiale.

Cisco 2600/3600 con ADSL-WIC e modulo di crittografia hardware è in grado di formare un Cisco 6160 Digital Subscriber Line Access Multiplexer (DSLAM). Cisco 6400 viene utilizzato come dispositivo di aggregazione per terminare una sessione PPP che viene avviata dal router Cisco 2600. Il tunnel IPSec ha origine sul CPE 2600 e termina sul Cisco 3600 nell'ufficio centrale, l'headend IPSec in questo scenario. Il dispositivo headend è configurato in modo da accettare connessioni da qualsiasi client anziché peer singoli. Il dispositivo headend viene inoltre testato solo con chiavi già condivise e codice HMAC (Message Authentication Code) basato su 3DES e Edge Service Processor (ESP)-Secure Hash Algorithm (SHA).



Configurazioni

Nel documento vengono usate queste configurazioni:

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

Tenere presente i seguenti punti relativi alle configurazioni:

- Viene utilizzata una chiave già condivisa. Per configurare sessioni IPSec per più peer, è necessario definire più istruzioni di definizione della chiave oppure configurare una mappa crittografica dinamica. Se tutte le sessioni condividono una singola chiave, è necessario utilizzare un indirizzo peer di 0.0.0.0.
- Il set di trasformazioni può essere definito per ESP, Authentication Header (AH) o entrambi per l'autenticazione doppia.
- Ènecessario definire almeno una definizione di criteri di crittografia per peer. Le mappe crittografiche determinano il peer da utilizzare per creare la sessione IPSec. La decisione si basa sulla corrispondenza dell'indirizzo definita nell'elenco degli accessi. In questo caso, è access-list 101.
- Le mappe crittografiche devono essere definite sia per le interfacce fisiche (in questo caso l'interfaccia ATM 0/0) sia per il modello virtuale.
- Nella configurazione illustrata in questo documento viene descritto solo un tunnel IPSec su una connessione DSL. Per evitare che la rete sia vulnerabile, sono probabilmente necessarie ulteriori funzionalità di sicurezza. Queste funzionalità di sicurezza possono includere elenchi di controllo di accesso (ACL) aggiuntivi, NAT (Network Address Translation) e l'utilizzo di un firewall con un'unità esterna o con un set di funzionalità del firewall IOS. Ognuna di queste funzionalità può essere utilizzata per limitare il traffico non IPSec da e verso il router.

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 - 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
!
```

Avvertenze

Le connessioni ADSL possono essere configurate con un modello virtuale o un'interfaccia di connessione.

Per configurare il CPE DSL in modo che riceva un indirizzo dal provider di servizi (l'indirizzo IP viene negoziato), viene utilizzata un'interfaccia dialer. Un'interfaccia di modello virtuale è un'interfaccia down-down e non supporta l'opzione dell'indirizzo negoziato, necessaria nell'ambiente DSL. Le interfacce con modelli virtuali sono state inizialmente implementate per gli ambienti DSL. Attualmente, un'interfaccia dialer è la configurazione consigliata sul lato DSL CPE.

Al momento della configurazione delle interfacce dialer con IPSec sono stati rilevati due problemi:

- ID bug Cisco CSCdu30070 (solo utenti registrati) —IPSec over DSL di solo software: cuneo della coda di input nell'interfaccia della connessione dialer DSL.
- ID bug Cisco CSCdu30335 (solo utenti registrati) —IPSec over DSL basato su hardware: cuneo della coda di input sull'interfaccia dialer.

Per risolvere entrambi i problemi, attualmente è necessario configurare CPE DSL con l'interfaccia del modello virtuale, come descritto nella configurazione.

Per entrambi i problemi, è prevista la risoluzione del software Cisco IOS versione 12.2(4)T. Dopo questa release, viene pubblicata una versione aggiornata di questo documento per mostrare la configurazione dell'interfaccia di connessione come un'altra opzione.

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Per verificare che la sessione IPSec sia stabilita tra i peer, è possibile utilizzare diversi comandi **show**. i comandi sono necessari solo sui peer IPSec, in questo caso Cisco serie 2600 e 3600.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

- **show crypto engine connections active**: visualizza tutte le associazioni di protezione per la fase 2 create e la quantità di traffico inviato.
- **show crypto ipsec sa**: visualizza la SA IPSec creata tra peer.

Di seguito viene riportato l'output del comando di esempio **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
```

In questo esempio viene restituito il 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:
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Il messaggio `"Modem state = 0x8"` segnalato dal comando **debug atm events** in genere indica che il WIC1-ADSL non è in grado di ricevere il rilevamento della portante dal DSLAM connesso. In questa situazione, il cliente deve controllare che il segnale DSL sia predisposto sui due cavi centrali rispetto al connettore RJ11. Alcune società di telefonia eseguono invece il provisioning del segnale DSL sui due pin esterni.

Comandi per la risoluzione dei problemi

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

Attenzione: non eseguire il debug su una rete attiva. Il volume delle informazioni visualizzate può sovraccaricare il router al punto in cui non vengono emessi flussi di dati e messaggi CPUHOG.

- **debug crypto IPSec**: visualizza gli eventi IPSec.
- **debug crypto Isakmp**: visualizza i messaggi sugli eventi IKE.

Riepilogo

L'implementazione di IPSec su una connessione ADSL garantisce una connessione di rete sicura e affidabile tra le filiali e i siti centrali. L'uso della serie Cisco 2600/3600 con i moduli ADSL-WIC e crittografia hardware offre al cliente costi di proprietà inferiori, in quanto è ora possibile utilizzare ADSL e IPSec in un'unica soluzione di router. La configurazione e le avvertenze elencate in questo documento devono servire come linee guida di base per impostare questo tipo di connessione.

Informazioni correlate

- Introduzione alla crittografia IP Security (IPSec)
- Cisco serie 2600 Router
- Reti private virtuali
- Supporto tecnico DSL e LRE
- Supporto dei prodotti gateway universali
- Supporto della tecnologia Dial and Access
- Supporto tecnico – Cisco Systems